Configuring and Managing Routers with Site Manager

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 117347-A Rev. A
September 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1997 Bay Networks, Inc.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, System 5000, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

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

Restricted Rights Legend

Use, duplication, or disclosure by the United States 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.

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

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. (“Bay Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Chapter 1
Getting Started with Site Manager

Chapter 2
Using the Configuration Manager

Chapter 3
Modifying and Saving Router Configurations

Chapter 4
Booting the Router

Chapter 5
Managing Router Files

Chapter 6
Customizing Router Software Images

Chapter 7
Monitoring Trap and Event Messages

Chapter 8
Monitoring Statistics

Chapter 9
Examining Configuration File Reports

Chapter 10
Auditing Configuration Files

Chapter 11
Using the Ping Option

Appendix A
Operating Site Manager with UNIX Commands

Appendix B
Site Manager Parameters

Appendix C
Checking SNMP SET Errors

Appendix D
Configuring the syslog Facility

Appendix E
Reallocating Memory Partitions for a Processor Module

Index

Figures

Tables

About This Guide

If you are responsible for configuring and managing routers with Site Manager, you need to read this guide.

If you want to	Go to
Start Site Manager	Chapter 1
Learn about the Configuration Manager	Chapter 2
Modify and save configuration files	Chapter 3
Boot the router	Chapter 4
Learn how to manage router files	Chapter 5
Modify router software images	Chapter 6
Monitor trap and event messages	Chapter 7
Monitor router statistics	Chapter 8
Generate a configuration file report or a binary configuration file	Chapter 9
Generate a configuration file audit trail	Chapter 10
Test the router connection using ping and the ping MIB	Chapter 11
Start Site Manager from the UNIX command line	Appendix A
Obtain Site Manager parameter descriptions	Appendix B
Learn about SNMP SET errors	Appendix C
Use the UNIX syslog facility to generate a configuration log	Appendix D
Reallocate memory partitions on FRE-2 and ACE-32 processor modules	Appendix E

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation guide that came with your router).
- Connect the router to the network (refer to *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7-11.xx to Version 12.00*.

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**

bold text

Indicates text that you need to enter, command names, and buttons in menu paths.
Example: Enter **wfsm &**

Example: Use the **dinfo** command.

Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.

italic text

Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.

quotation marks (“ ”)

Indicate the title of a chapter or section within a book.

`screen text`

Indicates data that appears on the screen.
Example: `Set Bay Networks Trap Monitor Filters`

separator (>)

Separates menu and option names in instructions and internal pin-to-pin wire connections.
Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.

Example: Pin 7 > 19 > 20

vertical line (|)

Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command.
Example: If the command syntax is

show at routes | **nets**, you enter either
show at routes or **show at nets**, but not both.

Acronyms

APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ATM	asynchronous transfer mode
BootP	Bootstrap Protocol
CLNP	Connectionless Network Protocol
GUI	graphical user interface
GMT	Greenwich mean time
IP	Internet Protocol
IPX	Internet Packet Exchange
ITU-T	International Telecommunications Union-Telecommunications (formerly CCITT)
LAN	local area network
MIB	management information base
NSAP	network service access point
OSI	Open Systems Interconnection protocol
PPP	Point-to-Point Protocol
RAM	random access memory
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

VINES	Virtual Network System
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	**Telephone number**	**Fax number**
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1
Getting Started with Site Manager

Site Manager is a software application for configuring and managing Bay Networks routers. It uses a graphical user interface (GUI) to make router configuration and management tasks easier. Site Manager is a collection of tools that enable you to perform the following tasks:

- Router configuration
- Software image building
- File management
- Router performance monitoring

You can operate Site Manager on a PC or a UNIX workstation, and integrate it with many popular Simple Network Management Protocol (SNMP) applications, such as the Hewlett-Packard OpenView Network Node Manager.

This chapter contains the following information:

(continued)

Before You Begin

If you are setting up a new router, complete the procedures that follow before continuing with this book. If your routers are already installed and operating, go to the next section, "How to Use This Guide."

For new routers, complete the following tasks:

- Boot the router according to the instructions in *Quick-Starting Routers.*

  Quick-Starting Routers is on the *Bay Networks BayRS Version 12.00 Online Library* CD for the current version of software. The CD is included with your router. These instructions start the router with a software image and a basic configuration file, which you can later modify to suit your network.

  At the end of the Quick-Start procedure, there are three configuration files on the router:

  -- *startup.cfg* (the Quick-Start procedure's suggested file name). This is the active file in the router's memory that configures the first interface on the router for the Internet Protocol (IP). The router is operating with this file at the end of the Quick-Start procedure.

  -- *ti.cfg*, the initial configuration file that contains only minimal information to boot new routers. You use *ti.cfg* before adding configuration information with the Quick-Start installation script. **Do not modify *ti.cfg* or overwrite it with another file.**

  -- *config*, the router's default configuration file. When you initially boot the router, *config* contains some system information, but it does *not* contain a configured router interface. When the router boots, it uses the *config* file by default.

- Install Site Manager as instructed in *Quick-Starting Routers*.

Updating the Original config File

The router uses the *config* file by default when it boots. When you first receive your router, the *config* file does not contain a configured router interface. You will need to update *config* to include a configured interface. To do this, modify *startup.cfg*, save the modified file under a unique name, then boot the router with this new file. If the router boots successfully, you can then save the new file under the name *config*.

For instructions on modifying router configuration files, refer to Chapter 3.

If you do not update the original default *config* file and the router reboots with this file, for example, after a power failure, it will not have a configured interface, making the router inaccessible using Site Manager. In this case, use the Technician Interface to reboot the router with *startup.cfg*, which will reactivate the initial network interface. The Technician Interface is a command-line interface that provides access to a Bay Networks router.

To access a router using the Technician Interface:

1. **Establish a Technician Interface session locally or with an out-of-band connection.**

   Refer to *Using Technician Interface Software.*

2. **Enter the following command:**

   boot <*slot_number***>:<***image_file***> <***slot_number***>:startup.cfg**

   For example:

   boot 2:bn.exe 2:startup.cfg

   The router boots and the IP initial interface is reestablished. You can now use Site Manager to access the router.

Router Security

As the system administrator responsible for configuring and managing your router, you need to have full read-write access to the router; however, you will want to prevent unauthorized users from accessing the router.

To secure the router, you must configure the router's SNMP agent so that specific routers belong to an SNMP community of the appropriate access level, that is, read or read/write.

If you have not already set up router security, refer to *Quick-Starting Routers* for instructions. For information about SNMP, refer to *Configuring SNMP, RMON, BootP, DHCP, and RARP Services*.

How to Use This Guide

Understanding how this guide is organized should make it more useful to you. The chapters are organized as follows:

- Getting Started with Site Manager

  If you are a new user, begin with this chapter. It tells you how to start Site Manager and familiarizes you with Site Manager's graphical user interface and its tools. If you are already familiar with Site Manager, skip this chapter and go to the chapter that best describes the task you are trying to accomplish.

- Descriptions of each Site Manager tool and the tasks that each tool helps you accomplish (Chapters 2 through 11)

  Go to the chapter that best describes the task you need to accomplish.

  If you are a new user, you will probably begin by configuring and booting the router, and performing basic file management. If you are an experienced user, you may be modifying your configuration, upgrading and loading new software, or monitoring router performance.

- Appendixes about starting Site Manager using UNIX commands, parameter descriptions, information about SNMP errors, the syslog facility, and reallocating memory partitions on processor modules.

The Site Manager windows in this guide are examples from a UNIX workstation. You may see slight differences if you are using Site Manager on a PC, but the windows work the same way.

Starting Site Manager

You should have already installed Site Manager on a UNIX workstation or a PC (see *Quick-Starting Routers* for instructions). The next step is to start Site Manager, according to instructions for your platform.

UNIX Workstation

Start Site Manager from a directory where you have read/write permissions, because this becomes the working directory for Site Manager operations. Do not start Site Manager from the */usr/wf* directory.

To start Site Manager:

1. **With a user account that has been set up for Site Manager, log on to a UNIX workstation.**

   Be sure that the user account has the correct environment variables set and that the workstation meets the system requirements for Site Manager (refer to *Quick-Starting Routers* for more information).

2. **Start the window environment.**

   Refer to the documentation for your UNIX workstation for instructions.

3. **Go to the directory where you want to store router configuration files.**

4. **Enter wfsm &**

   Site Manager starts and the Router Connection Options window opens (Figure 1-1). From this window, you will connect to the router. Go to "Connecting to a Router for the First Time."

   You can also start Site Manager from the UNIX command line, but this method is only recommended for users experienced with Site Manager. Refer to Appendix A for instructions.

PC

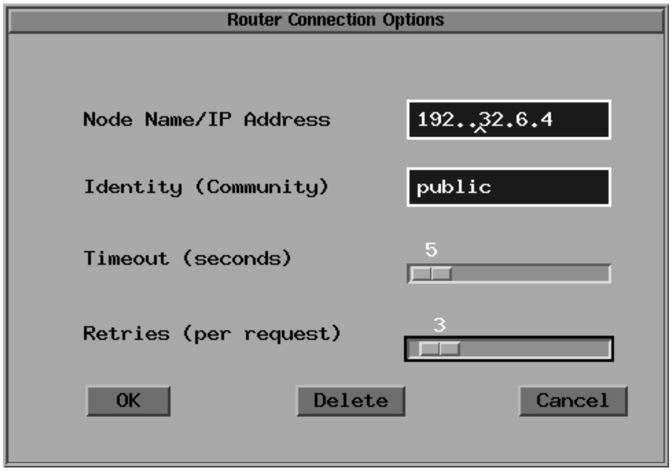
To start Site Manager using Windows 95®:

1. **From the Windows 95 desktop, click on the START button.**
2. **From the START menu, choose Programs > Site Manager > PC_Site Manager.**

   The main Site Manager window opens, then the Router Connection Options window opens (Figure 1-1). From this window, you connect to the router. Go to "Connecting to a Router for the First Time."

Connecting to a Router for the First Time

The first time you start Site Manager, the Router Connection Options window opens, prompting you to define a router connection (Figure 1-1).



Router Connection Options

Node Name/IP Address 192.32.6.4

Identity (Community) public

Timeout (seconds) 5

Retries (per request) 3

Figure 1-1. Router Connection Options Window

The Router Connection Options window lets you connect to a Bay Networks router. You can open this window from within different Site Manager tools and connect to a different router. In this way, you can manage several routers at the same time.

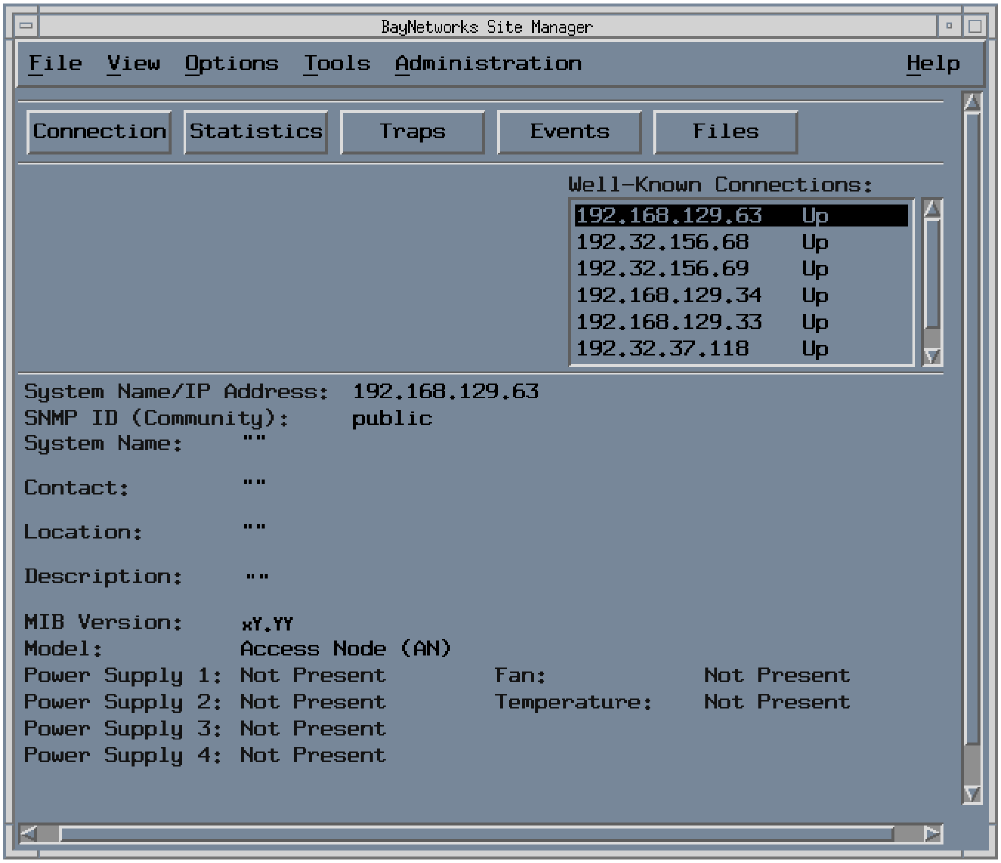
To connect to a router:

1. **Type the IP address of the router you want to connect to.**
2. **Accept the default values for the remaining fields in the window or supply new values. See the parameter descriptions beginning on page B-2.**

   You can click on Delete to delete the currently displayed connection.
3. **Click on OK.**

   Site Manager connects to the router and opens the main Site Manager window (Figure 1-2).

   It also adds the router's IP address to the Well-Known Connections list, on the right side of the main Site Manager window.



```
Well-Known Connections:
192.168.129.63    Up
192.32.156.68     Up
192.32.156.69     Up
192.168.129.34    Up
192.168.129.33    Up
192.32.37.118     Up

System Name/IP Address:  192.168.129.63
SNMP ID (Community):     public
System Name:      ""

Contact:          ""

Location:         ""

Description:      ""

MIB Version:      xY.YY
Model:            Access Node (AN)
Power Supply 1:  Not Present          Fan:            Not Present
Power Supply 2:  Not Present          Temperature:    Not Present
Power Supply 3:  Not Present
Power Supply 4:  Not Present
```

Figure 1-2. Bay Networks Site Manager Window

Main Site Manager Window

Site Manager’s graphical user interface organizes, summarizes, and simplifies router information. The first window you see after you start Site Manager is the main Site Manager window (refer to Figure 1-2). You access all Site Manager tools and commands from the main window. The lower half of the window displays basic router information such as IP address, SNMP community, system name, and management information base (MIB) version.

The next sections describe each part of the main Site Manager window.

Main Menu Bar

The Site Manager main menu bar lets you access the following options (Figure 1-3):

- File - exits Site Manager
- View - refreshes the Site Manager display
- Options - enables you to connect to routers and define connection options
- Tools - lets you access all Site Manager tools
- Administration - lets you select administration functions, such as booting and setting the router’s date and time
- Help - indicates the version of Site Manager you are operating

Subsequent sections in this chapter explain how to use each option.

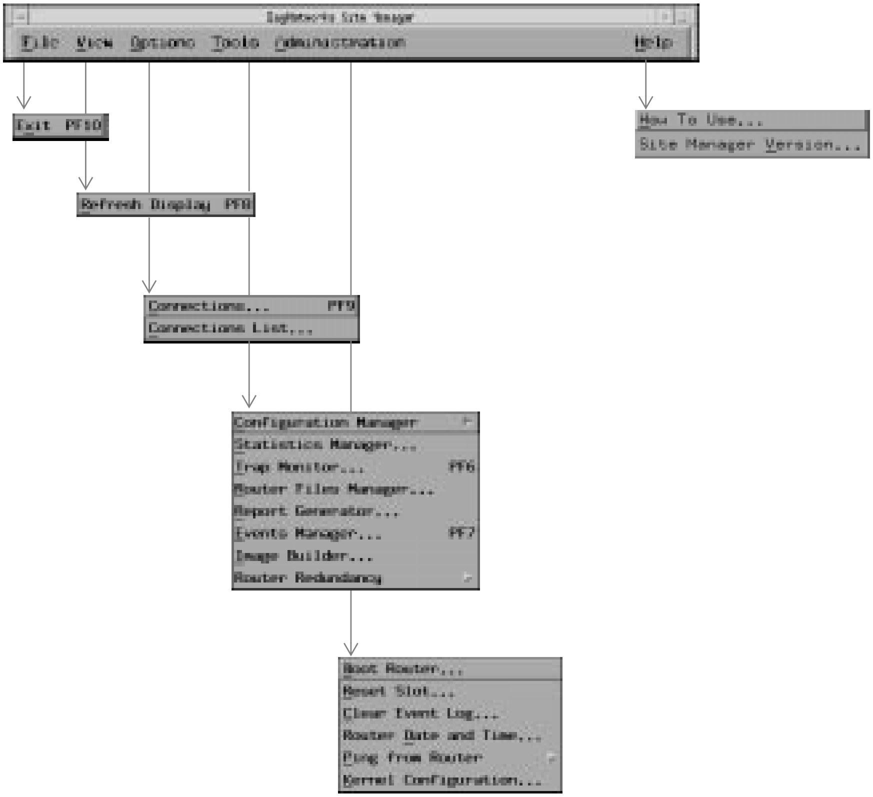


Figure 1-3. Main Menu Bar and Submenus

Main Window Buttons

Below the main menu bar is a row of buttons that let you access certain Site Manager functions (Figure 1-4).

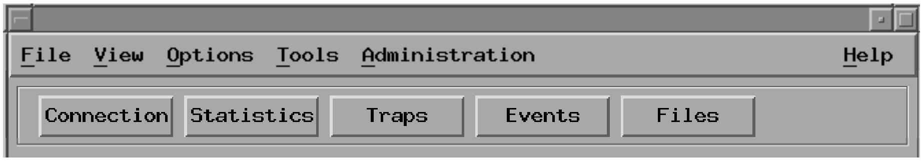


Figure 1-4. Buttons on the Main Site Manager Window

Table 1-1 describes each button.

Table 1-1. Main Window Buttons

Button	Function
Connection	Opens the Router Connection Options window, which lets you connect to a specific rout and delete router entries.
Statistics	Opens the Statistics Manager window. Refer to Chapter 8 for more information about the Statistics Manager.
Traps	Opens the Trap Monitor window. Refer to Chapter 7 for more information about the Trap Monitor.
Events	Opens the Events Manager window. Refer to Chapter 7 for more information about the Events Manager.
Files	Opens the Router Files Manager window. Refer to Chapter 5 for more information about the Router Files Manager.

The windows that you access using a button are also accessible from the Options or Tools menu on the main menu bar.

Well-Known Connections List

At the right of the main Site Manager window, there is a list box entitled Well-Known Connections (refer to Figure 1-2), which lists the IP addresses of routers you have connected to with this version of Site Manager. Click on an IP address in the list to connect to a specific router.

For information about how to use this list, go to "Connecting to Routers" on page 1-16.

Using Site Manager Windows

To use Site Manager, you need to learn about:

- Site Manager menu bars and function buttons
- Site Manager window conventions
- Getting Help for Site Manager windows

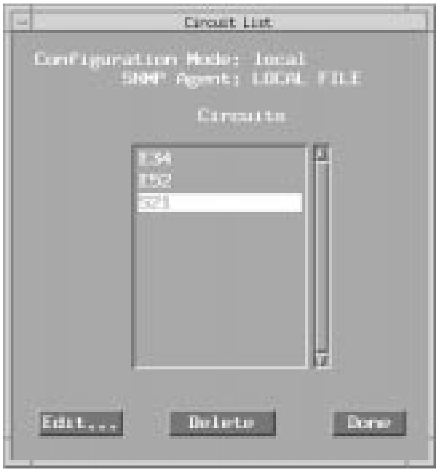
To configure your router, you use the Configuration Manager. Refer to Chapter 2 for information about the Configuration Manager and how to enter data in the Configuration Manager windows.

Menu Bars and Function Buttons

Every Site Manager window has either a menu bar or function buttons.

A *menu bar* lets you access additional menus and commands. For example, the Site Manager main menu bar (refer to Figure 1-3) gives you access to the File, View, Options, Tools, and Administration menus.

Function buttons let you enter and modify data for a specific function. For example, the Circuit List window (Figure 1-5) contains Edit, Delete, and Done buttons. You use the Edit button to edit a circuit, the Delete button to delete a circuit, and the Done button to close the Circuit List window.



Configuration Mode: local
SNMP Agent: LOCAL FILE

E34
E52
S21

Figure 1-5. Window with Function Buttons

Window Conventions

Site Manager windows use the following conventions:

- Menu options and buttons that end with three dots (...) display a window when you select them.
- Menu options not followed by three dots and menu options followed by a shaded arrow (▶) display a menu when you select them.
- Buttons not followed by three dots perform a function when you click on them.
- Underlined letters in menu options identify keyboard shortcuts.
  - -- If you are using a Sun or IBM keyboard, hold down the meta key (on either side of the space bar) and press the key underlined in the menu option to select that option.
  - -- If you are using a PC keyboard, hold down the [Alt] key and press the key underlined in the menu option to select that option.
- The arrow keys on the keyboard allow you to scroll up, down, right, or left within a menu.
- The PF number in a menu option identifies the program function key shortcut. This number appears to the right of an option in a menu (refer to Figure 1-3).
- Menu options are dimmed when they are not active for a particular window.
- Some Site Manager windows have vertical scroll bars at the right side of the window. You can view the entire contents of a window using the scroll bar.

Getting Help for Site Manager Windows

Some Site Manager windows have a Help button near the bottom of the window. By clicking on this button, you receive instructions about the window itself. Figure 1-6 shows the Trap Configuration window with a Help button.

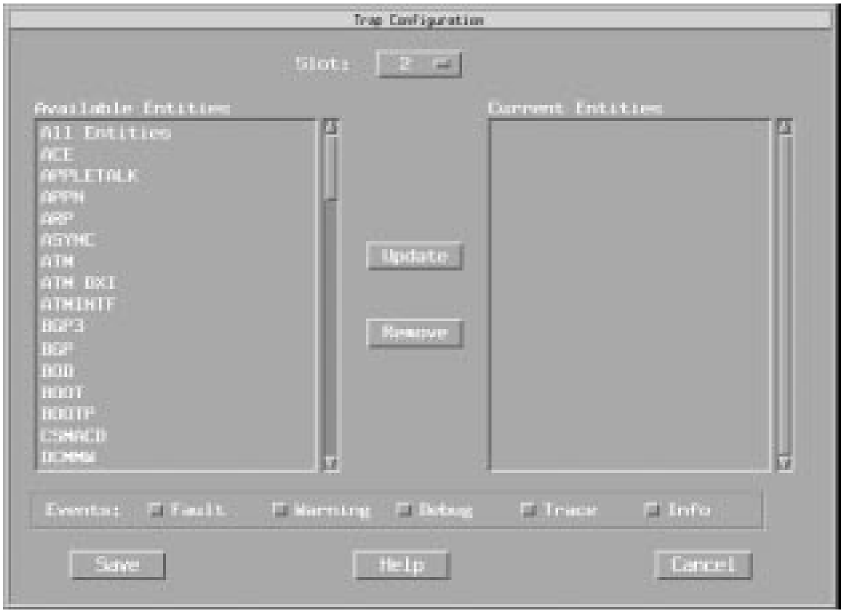
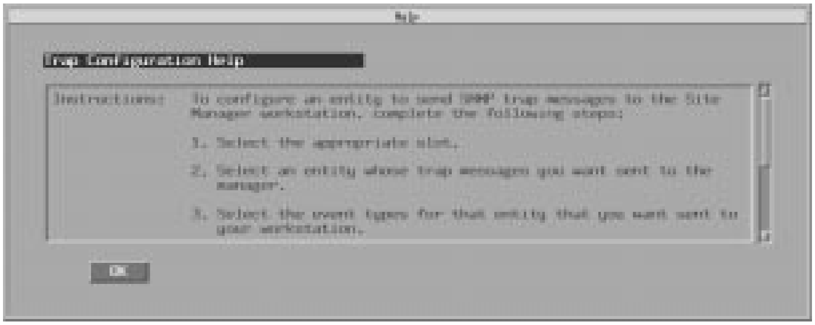


Figure 1-6. Trap Configuration Window with Help Button

To get Help about the window, click on Help; a Help window opens (Figure 1-7).



Instructions: To configure an entity to send SNMP trap messages to the Site Manager workstation, complete the following steps:

1. Select the appropriate slot.
2. Select an entity whose trap messages you want sent to the manager.
3. Select the event types for that entity that you want sent to your workstation.

Figure 1-7. Trap Configuration Help Window

To exit the Help window, click on OK.

Performing Basic Site Manager Operations

This section describes the following basic operations you can perform with Site Manager:

- Connecting to routers
- Setting the router's date and time
- Determining Site Manager version
- Starting Site Manager tools
- Exiting Site Manager tools

Connecting to Routers

When you connect to a router for the first time, you must enter the router's IP address in the Router Connection Options window (refer to "Connecting to a Router for the First Time" on page 1-7).

For subsequent connections, you can use any one of the following methods to connect to a router:

- Router Connection Options window
- Well-Known Connections list
- Options function from within a Site Manager tool

The next sections describe each router connection method. These methods allow you to connect to one router at a time. You can also connect to multiple routers when transferring files using the Router Files Manager tool. Refer to Chapter 5 for instructions.

Using the Router Connection Options Window

To access the Router Connection Options window:

1. **In the main Site Manager window (refer to Figure 1-2), click on the Connection function button or choose Options > Connections.**

   The Router Connection Options window opens (refer to Figure 1-1).

2. **In the Node Name/IP Address field, type the IP address of the destination router.**

3. **Accept the default values for the remaining parameters in the window or supply new values. See the parameter descriptions on page B-2.**

   You can click on Delete to delete the currently displayed connection.

4. **Click on OK.**

   Site Manager connects to the router. The connection is successful if the router's system information is displayed in the lower half of the main Site Manager window.

Using the Well-Known Connections List

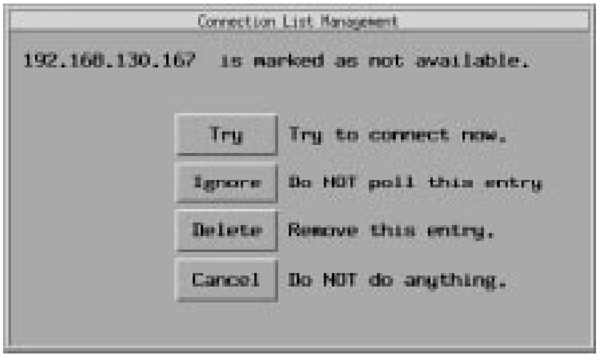
At the right of the main Site Manager window, there is a list box entitled Well-Known Connections (refer to Figure 1-2), which lists the IP addresses of routers you have already connected to with this version of Site Manager.

To connect to a specific router, simply click on the router's IP address, and Site Manager makes the connection. This method is the easiest way to connect to a router.

Site Manager lists the IP addresses in numeric order. Every time you make a new connection using the Connection button or the Router Connection Options window, Site Manager automatically adds the new IP address to the Well-Known Connections list. You can have a maximum of 50 addresses in the list.

The status of the connection to the router is polled at a rate you can define. The Well-Known Connections window displays the results of the poll next to the IP address, as Up, Down, or Ignore.

If you click on an IP address listed as Down, the Connection List Management window opens (Figure 1-8).



Connection List Management

192.168.130.167 is marked as not available.

Try to connect now.

Do NOT poll this entry

Remove this entry.

Do NOT do anything.

Figure 1-8. Connection List Management Window

Table 1-2 describes the options in the Connection List Management window.

Table 1-2. Options in Connection List Management Window

Option	Function
Try	Polls the accessibility of the connection to the router again, and tries to connect to the router
Ignore	Does not poll the address again
Delete	Removes the address from the Well-Known Connections list
Cancel	Returns to the previous window without changing anything

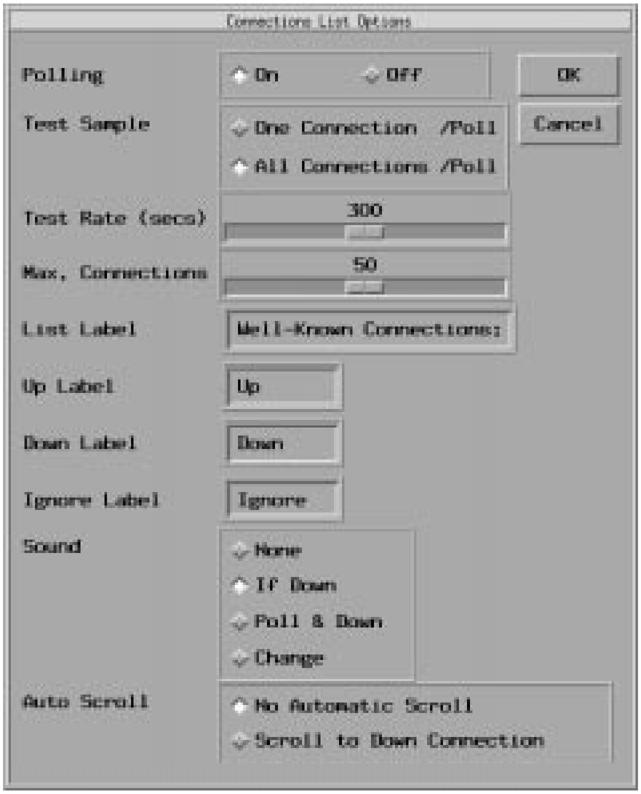
Click on the option you want for this connection. You then return to the main Site Manager window.

Configuring the Well-Known Connections List

You can define how Site Manager displays information in the Well-Known Connections list, how many routers are in the list, as well as other connection features.

To set the options you want in the Well-Known Connections list, choose Options > Connections List from the Site Manager menu.

The Connections List Options window opens (Figure 1-9).



Connections List Options

Polling ◆ On ◇ Off

Test Sample ◇ One Connection /Poll ◆ All Connections /Poll

Test Rate (secs) 300

Max. Connections 50

List Label Well-Known Connections:

Up Label Up

Down Label Down

Ignore Label Ignore

Sound ◇ None ◆ If Down ◇ Poll & Down ◇ Change

Auto Scroll ◆ No Automatic Scroll ◇ Scroll to Down Connection

Figure 1-9. Connections List Options Window

Table 1-3 describes the options in the Connections List Options window.

Table 1-3. Connections List Options

Option	Function
Polling	Enables or disables the polling of the IP addresses in the list. If you set this option to On, Site Manager polls the IP addresses in the Well-Known Connections list to test whether the connections are still accessible.
Test Sample	Tests one connection or all connections per poll. If you select One Connection, each poll tests one connection on the list in sequential order.
Test Rate (secs)	Specifies how often to poll the IP addresses to test the validity of the connections. The default is 300 seconds.
Max. Connections	Sets a maximum number of IP addresses displayed in the Well-Known Connections list. The maximum number of address entries is 50. If you set this field to a value less than the number of connections currently in the list, Site Manager truncates the list from the bottom.
List Label	Lets you change the label (or name) of the Well-Known Connections list.
Up Label	Lets you change the label indicating the status of an accessible IP address in the Well-Known Connections list.
Down Label	Lets you change the label indicating the status of an inaccessible IP address in the Well-Known Connections list.
Ignore Label	Lets you change the label indicating the status of connections to be ignored in the Well-Known Connections list. Site Manager does not poll ignored connections.
Sound	Specifies when (if at all) the Well-Known Connections list generates a sound. The list can generate a sound when: • A connection is down (the default). • Polling occurs (one beep) and polling shows that a connection is down (one beep per down connection). • There is a change in status.
Auto Scroll	Lets you specify whether you want Site Manager to automatically scroll to a down connection in the Well-Known Connections list.

When you complete your changes in the Connections List Option window, click on OK to implement them.

Connecting to the Router from a Site Manager Tool

Several Site Manager tools (the Router Files Manager, the Statistics Manager, and the Events Manager) let you connect to a router from within the tool.

To connect to a router from a Site Manager tool:

1. **Select Tools > <*tool option*>.**

   The tool's main window opens.

2. **Choose Options > Router Connection.**

   The Router Connection Options window opens (refer to Figure 1-1).

3. **Specify the destination router's IP address in the Node Name/IP Address field.**

4. **Click on OK.**

The router's IP address is displayed in the tool's main window while the connection is active.

Router Connection Messages

Site Manager provides three error messages that explain why a router connection attempt failed. These messages tell you what adjustments are needed to connect to the router. Any of these messages can appear in a message window in response to a failed connection attempt (Table 1-4).

Table 1-4. Router Connection Error Messages

Error Message	**Meaning and Action**
Connection failed, SNMP agent not responding. Check IP address and Community. Timeout and Retries may also need to be increased.	The router at the specified IP address did not respond to the connection attempt from your Site Manager workstation. Check the IP address, Community, Timeout, and Retries settings.
WARNING: Site Manager no longer supports the version of software that the router is running. Proceed with caution.	The router at the specified IP address is using a MIB version that is older than the MIB versions that your Site Manager workstation supports. (There is a backward-compatibility problem.) Update the router software to an appropriate version.
WARNING: Site Manager has discovered a forward compatibility situation with the router software. It is recommended that Site Manager be upgraded in order to manage this router properly. Proceed with caution.	The router at the specified address is using a MIB version that is newer than the MIB versions that your Site Manager workstation supports. (There is a forward-compatibility problem.) Upgrade Site Manager software.

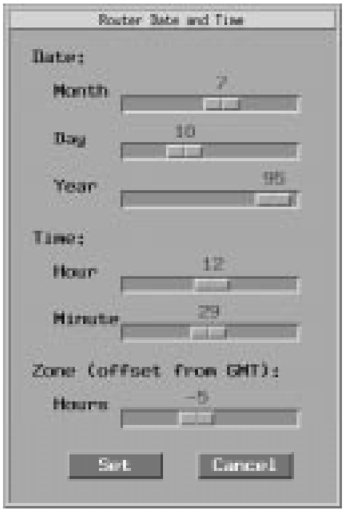
Setting a Router’s Date and Time

To update the router’s date, time, and time zone, use the Router Date and Time option.

To update the routers date, time, and time zone:

1. **In the main Site Manager window, choose Administration > Router Date and Time.**

   The Router Date and Time window opens (Figure 1-10).



Router Date and Time

Date:

Month 7

Day 10

Year 95

Time:

Hour 12

Minute 29

Zone (offset from GMT):

Hours -5

Figure 1-10. Router Date and Time Window

2. **Use the slide bar in each field to select the correct values.**

   The Zone field lets you specify the number of hours your time zone is ahead of or behind Greenwich mean time (GMT). Move the slide bar to the left to select a value behind (-) GMT. Move the slide bar to the right to select a value ahead of GMT. For example, Eastern Standard Time is 5 hours behind GMT, so you would select -5.

3. **Click on Set.**

   The information is saved and you return to the main Site Manager window.

Displaying Site Manager Version

To display the version of Site Manager you are running, choose Help > Site Manager Version in any window. The Version window opens (Figure 1-11).

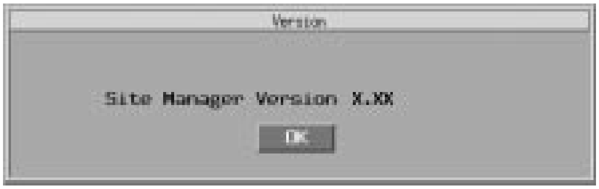


Figure 1-11. Version Window

Make sure that the Site Manager version is compatible with the version of router software shown in the Description and MIB Version fields in the lower half of the main Site Manager window (refer to Figure 1-2). If you have questions about Site Manager and router software compatibility, check the Release Notes for the router software or contact the Bay Networks Technical Solutions Center.

Starting Site Manager Tools

To start a Site Manager tool, choose an option from the Tools menu in the main Site Manager window (refer to Figure 1-3). Table 1-5 lists and describes Site Manager tools.

Table 1-5. Site Manager Tools

Site Manager Tool	What It Does
Configuration Manager	Configures the router.
Statistics Manager	Collects information about the router, protocols, the MIB, and router performance.
Trap Monitor	Collects real-time information about the operating status of the router.
Router Files Manager	Transfers, copies, deletes, and manages files.
Report Generator	Creates reports about router configuration files.
Events Manager	Displays the current event log, which includes detailed messages about the operating status of the router.
Image Builder	Customizes router software image files.
Router Redundancy	Enables you to configure a router as a backup router and include it in a *router redundancy group*. If a primary router from the redundancy group fails, a secondary router activates. If you want to configure a router with the redundancy feature, use this option instead of the Configuration Manager. Refer to *Configuring Interface and Router Redundancy* for all configuration instructions.

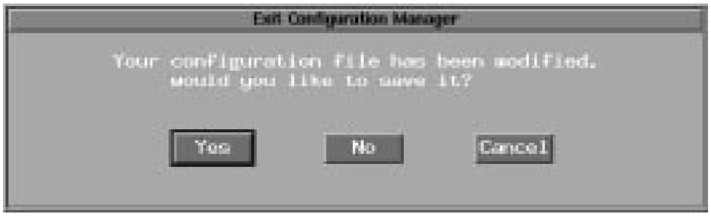
Each of these tools, except router redundancy, is described in a subsequent chapter of this guide. For information about starting Site Manager tools from the UNIX command line, refer to Appendix A.

For information about router redundancy, refer to *Configuring Interface and Router Redundancy.*

Exiting Site Manager Tools

To exit a Site Manager tool, begin at the main window for the tool and choose File > Exit.

For all tools other than the Configuration Manager, you exit the tool immediately. If you are exiting the Configuration Manager, a window opens (Figure 1-12) asking:



Exit Configuration Manager

Your configuration file has been modified.
would you like to save it?

Figure 1-12. Exit Configuration Manager Window

Click on Yes to save your changes and exit the Configuration Manager. Click on No to exit the Configuration Manager without saving your changes, or click on Cancel to continue.

Caution: When you exit a Site Manager window on the PC, always use the appropriate Site Manager button or menu. Do not exit a Site Manager window using the Windows 95 Close button in the upper right corner of each window because you may affect Site Manager operation.

All windows associated with the tool close when you shut down the application.

Exiting Site Manager

➡ **Caution:** When you exit a Site Manager window on the PC, always use the appropriate Site Manager button or menu. Do not exit a Site Manager window using the Windows 95 Close button in the upper right corner of each window because you may affect Site Manager operation.

To exit Site Manager:

1. **Access the main Site Manager window (refer to Figure 1-2).**
2. **Choose File > Exit.**

   A confirmation window opens asking if you want to exit.
3. **Click on OK.**

When you exit Site Manager on a UNIX workstation, only those tools and associated windows you started from the Site Manager window shut down. Tools started from the command line remain open.

When you exit Site Manager on a PC, a window indicates which Site Manager tools and associated windows are still open. You cannot exit Site Manager until you close these windows.

Changing Site Manager Fonts and Colors

To display and change Site Manager fonts and colors, go to one of the following sections:

- Changing Fonts on a PC
- Changing Colors on a PC
- Changing Fonts on a UNIX Workstation
- Changing Colors on a UNIX Workstation

Changing Fonts on a PC

To change Site Manager fonts on the PC, open the file *jam.ini* in your Windows 95 directory (usually *\windows*). Search for the following line:

```
SystemFont=OEM_FIXED_FONT
```

Change `OEM_FIXED_FONT` to the font you want. The *jam.ini* file provides examples. A sample change follows:

```
SystemFont=SYSTEM_FIXED_FONT
```

Changing Colors on a PC

The color scheme of Windows 95 determines the colors displayed in Site Manager windows. To change the colors, refer to the documentation for Windows 95.

Caution: Do not edit the colors defined in the *jam.ini* file; this may cause problems with Site Manager.

Changing Fonts on a UNIX Workstation

You can change fonts and colors for yourself or for all users of Site Manager on a UNIX workstation.

The *.Xdefaults* file in your home directory defines the fonts and colors for your Site Manager environment.

The *XJam* file defines Site Manager fonts and colors displayed in windows for all users of Site Manager. On SPARCstations running OpenWindows, this file is in the *$OPENWINHOME/lib/app-defaults* directory. On SPARCstations running X11, and on HP 9000 and RS/6000 workstations, this file is in the */usr/lib/X11/app-defaults* directory.

When changing a font or color, make sure that your system supports the new font or color. Refer to the documentation that came with your system.

To change the font for your own use of Site Manager:

1. **Add the following line to your *.Xdefaults* file, where *font* is the name of the font you want:**

   XJam*fontList:*font*

2. **Save the *.Xdefaults* file.**
3. **Enter the following command to reload the contents of the *.Xdefaults* file on the X server:**

   ```
   xrdb  -merge .Xdefaults
   ```

To change the font for all users of Site Manager on this workstation:

1. **Open the *XJam* file.**
2. **Search for the following line:**

   ```
   XJam*fontList:8x13
   ```

3. **Change `8x13` to the font you want.**
4. **Save the *XJam* file.**

Changing Colors on a UNIX Workstation

To change the foreground or background color for your own use of Site Manager:

1. **Add the appropriate line to the *.Xdefaults* file.**

   If you want to change the foreground color, add the following line, where *color* is the name of the color you want:

   XJam*foreground:*color*

   If you want to change the background color, add the following line, where *color* is the name of the color you want:

   XJam*background:*color*

2. **Save the *.Xdefaults* file.**

3. **Enter the following command to reload the contents of the *.Xdefaults* file on the X server:**

   xrdb -merge.Xdefaults

To change the foreground or background color for all users of Site Manager on this workstation:

1. **Open the *XJam* file.**

2. **Search for the appropriate line, as follows:**

   If you want to change the foreground color, search for the following line:

   ```
   XJam*foreground:steelblue3
   ```

   If you want to change the background color, search for the following line:

   ```
   XJam*background:chartreuse3
   ```

3. **Change the color name to the one you want.**

4. **Save the *XJam* file.**

Chapter 2
Using the Configuration Manager

This chapter describes the Configuration Manager, the Site Manager tool that lets you create and modify router configuration files.

A configuration file contains the user-defined configuration for a router and its interfaces. Once you have a working configuration file, you can use that file to boot the router.

➡ **Note:** If you are configuring an Access Node (AN®), Access Node Hub (ANH™), Access Stack Node (ASN™), or Advanced Remote Node™ (ARN™) for the first time, you must read *Configuring BayStack Remote Access* or *Connecting ASN Routers to a Network* before you continue. These guides explain the special considerations for configuring and booting ANs, ANHs, ARNs, and ASNs.

This chapter contains the following information:

Topic	Page
Configuration Manager User Interface	2-2
Configuration Manager Operating Modes	2-8
The Configuration Manager and the Technician Interface	2-22

Instructions for modifying and saving configuration files are in Chapter 3.

Configuration Manager User Interface

The Configuration Manager is the tool you use to configure a router. You access the Configuration Manager by choosing Tools > Configuration Manager from the main Site Manager window.

Using the Configuration Manager, you can do the following:

- Customize and add network interfaces on the router.
- Make configuration changes locally or remotely.
- Configure the router’s connection to the Technician Interface.

Each Configuration Manager session allows you to access only one router. To configure two routers simultaneously, first connect to one router and bring up the Configuration Manager. Then, return to the main Site Manager window, open the Router Connection Options window, connect to the second router, and start another Configuration Manager session.

Before you perform any of the configuration tasks, you need to familiarize yourself with the Configuration Manager interface. The following sections explain how to enter data in the Configuration Manager windows:

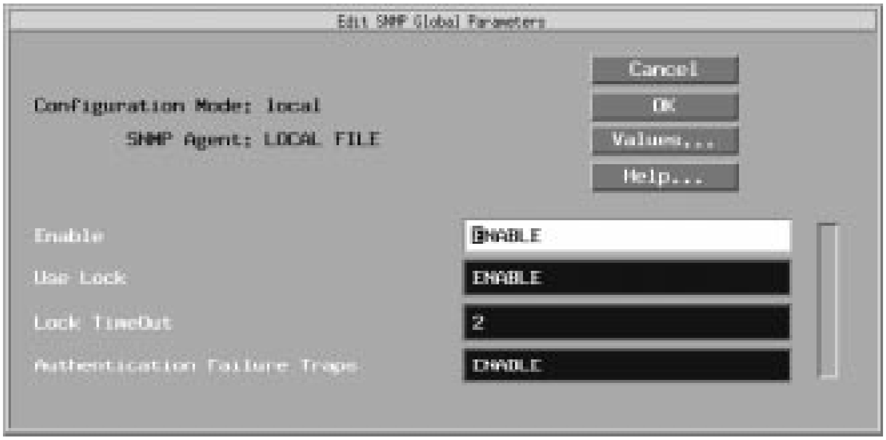
- Entering Parameter Values Using the Values Button on page 2-3
- Entering Parameter Values Using the Keyboard on page 2-4
- Getting Help for Parameters on page 2-5

After you are familiar with how to enter configuration data, you can learn about the Configuration Manager’s three operating modes.

Entering Parameter Values Using the Values Button

To configure a router, you need to enter values for parameters in the Configuration Manager windows. Most configuration parameters have a default value that is displayed in the parameter field. To change the default value, you can use the Values button and choose a value from a list of valid options. The Values button is in the upper right corner of the window (Figure 2-1). This is the recommended method for selecting parameter values.

➡ **Note:** Some parameters do not list options when you click on Values, for example, an IP address parameter or a password parameter. You must type such values.



Configuration Mode: local
SNMP Agent: LOCAL FILE

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

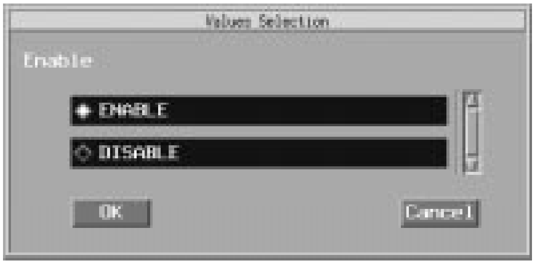
Figure 2-1. Edit SNMP Global Parameters Window

To select a parameter value using the Values button:

1. **Click on the field across from the parameter.**
2. **Click on Values.**

   The Configuration Manager opens a Values Selection window that lists all valid options for that parameter.

   Figure 2-2 shows an example for the Enable parameter in the Edit SNMP Global Parameters window.



Values Selection

Enable

◆ ENABLE

◇ DISABLE

Figure 2-2. Values Selection Window

3. **Click on the diamond to the left of the option you want.**
4. **Click on OK.**

   The option you selected appears in the appropriate field. Click on Cancel to exit the Values Selection window without choosing a value. Exit the Values Selection window to view values for other parameters.

Entering Parameter Values Using the Keyboard

You can also use the keyboard to enter parameter values.

To replace an existing value for a parameter:

1. **Place the cursor in the parameter field.**
   - Double-click on a word to select the word only.
   - Triple-click on a word to select the entire field.
2. **Type a new value.**

To add to the existing value or to overwrite the value:

1. **Place the cursor in the parameter field.**
2. **Toggle the insert key to either *insert* or *overwrite* mode.**
   - In insert mode, the cursor appears as an I (I), and your entry is added to the existing entry.
   - In overwrite mode, the cursor appears as a block (▯), and your entry overwrites the existing entry.
3. **Type a new value.**

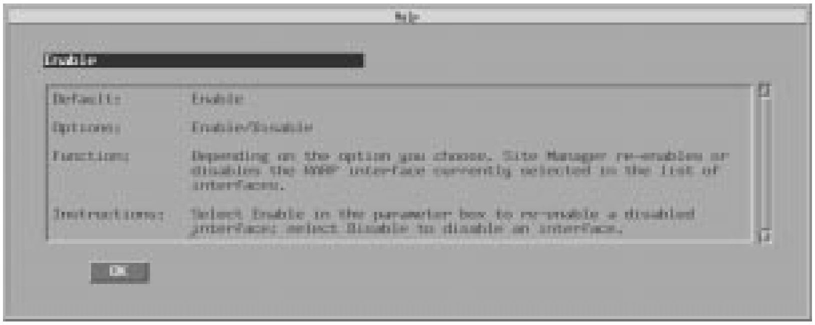
Getting Help for Parameters

Most Configuration Manager windows have a Help button in upper right corner of the window (refer to Figure 2-1). If you are unsure of a parameter's function, click on Help to get a description of the parameter that includes the default value, the valid options, the function of the parameter, and instructions about setting the parameter.

To get help about a parameter:

1. **Click in the field for which you want help.**
2. **Click on Help.**

   For example, if you click in the Enable field in the Edit SNMP Global Parameters window (refer to Figure 2-1) then click on Help, a Help window opens (Figure 2-3).



```
Default:        Enable
Options:        Enable/Disable
Function:       Depending on the option you choose, Site Manager re-enables or
                disables the SNMP interface currently selected in the list of
                interfaces.
Instructions:   Select Enable in the parameter box to re-enable a disabled
                interface; select Disable to disable an interface.
```

Figure 2-3. Enable Parameter Help Window

Use the scroll bar on the right side of the window to read the entire help text. Click on OK to close the window. You must close a Help window before you can get Help for other parameters.

Specifying System Information

When you connect to the router from the main Site Manager window, Site Manager displays administrative information in the main Site Manager window (refer to Figure 1-2).

You can use the Configuration Manager to specify a system name, a system contact, and a system location for the router.

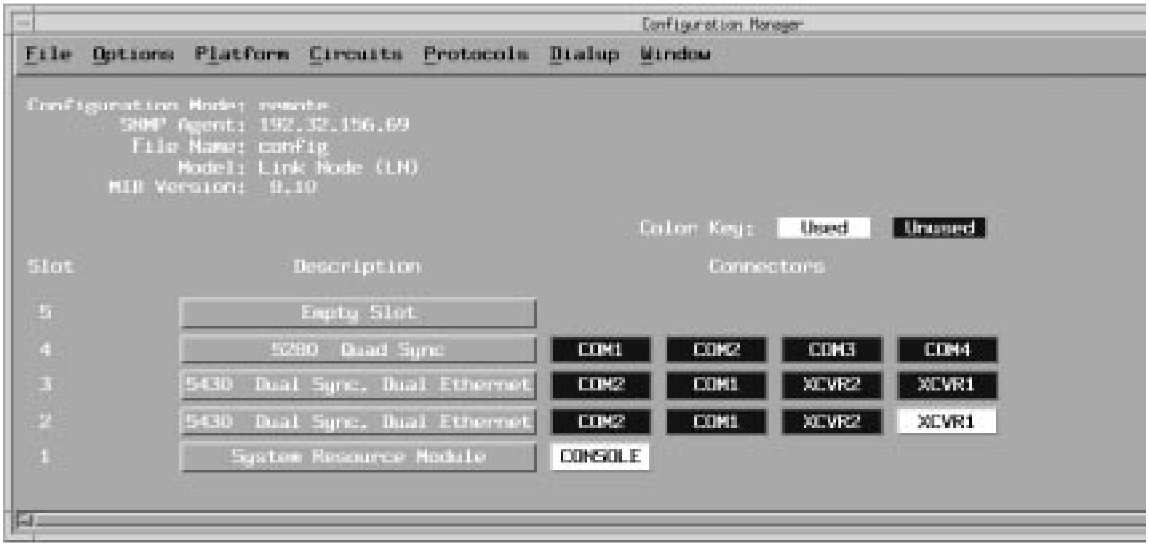
To specify router information:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Configuration Manager > Local File/Remote File/Dynamic.**

   The Configuration Manager window opens (Figure 2-4).



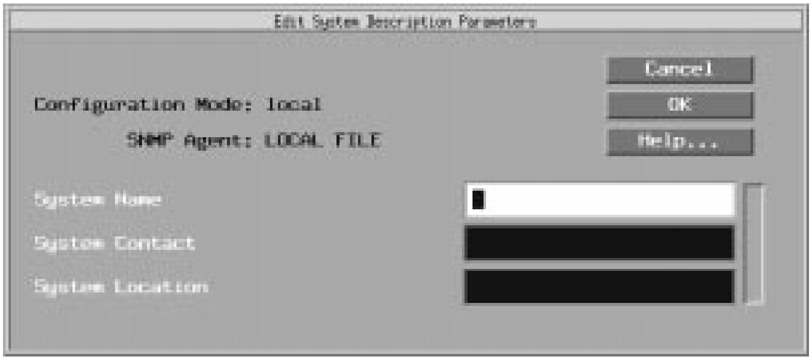
```
Configuration Mode: remote
        SNMP Agent: 192.32.156.69
         File Name: config
             Model: Link Node (LN)
       MIB Version:  8.10
```

Slot	Description	Connectors			
5	Empty Slot				
4	5280 Quad Sync	COM1	COM2	COM3	COM4
3	5430 Dual Sync, Dual Ethernet	COM2	COM1	XCVR2	XCVR1
2	5430 Dual Sync, Dual Ethernet	COM2	COM1	XCVR2	XCVR1
1	System Resource Module	CONSOLE			

Figure 2-4. Configuration Manager Window

3. **Choose Platform** > **Edit System Information.**

   The Edit System Description Parameters window opens (Figure 2-5).



Edit System Description Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

Figure 2-5. Edit System Description Parameters Window

4. **Enter the required information.**

   Refer to the parameter descriptions beginning on page B-4. You can also click on Help.

5. **Click on OK.**

   The information is saved and you return to the Configuration Manager window.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

7. **Do one of the following to see the new system information:**

   a. **For local and remote configuration files, you will not see the new information until you reboot the router. For instructions on booting the router, refer to Chapter 4.**

   b. **For dynamic configurations, select View > Refresh from the main Site Manager menu bar to see the new system information.**

Configuration Manager Operating Modes

You can perform all configuration tasks in one of three modes:

- Local mode, described on page 2-8
- Remote mode, described on page 2-19
- Dynamic mode, described on page 2-21

The Configuration Mode field in the upper left corner of each window identifies the Configuration Manager's current operating mode (refer to Figure 2-4). The Configuration Manager displays the same windows in the same sequence regardless of the operating mode.

Local Mode

Local mode lets you create or edit a configuration file locally on the Site Manager workstation for later implementation on the router. Unlike remote and dynamic modes, local mode does not access a router or, for new configurations, automatically display the router's hardware configuration. You enter the router's hardware configuration when you create a new configuration file or edit a file with hardware changes.

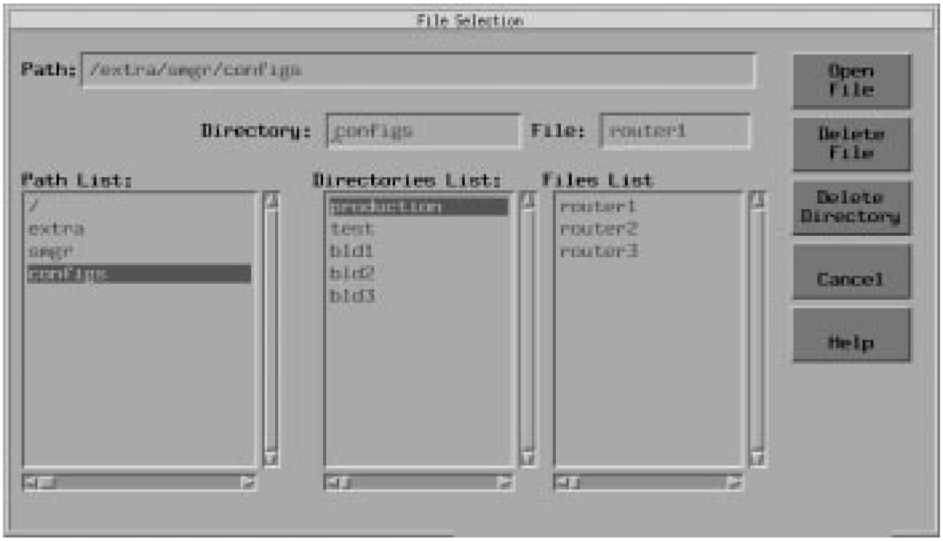
Local mode is the most cautious mode in which to work. In this mode, you do not edit the configuration file in RAM or in permanent storage until you transfer the file to the router and boot with that file.

You can create a new configuration file or open an existing one in local mode. If you are modifying an existing configuration file, you can use a copy of the file residing on the Site Manager workstation or use the Router Files Manager to transfer a copy of a file from the router to the Site Manager workstation. For instructions about using the Router Files Manager, refer to Chapter 5.

➡ **Note:** In local mode, you can only create new configurations for the current version of software; however, you can modify existing configurations from previous versions.

Opening a Configuration File in Local Mode

To open a configuration file in local mode, begin at the main Site Manager window and choose Tools > Configuration Manager > Local File. The File Selection window opens (Figure 2-6).



Path: /extra/smgr/configs

Directory: configs File: router1

Path List:
/
extra
smgr
configs

Directories List:
production
test
bld1
bld2
bld3

Files List
router1
router2
router3

Figure 2-6. File Selection Window

The File Selection window contains the following information:

- The *Path List*, which shows the path from the root directory to the current directory.
- The *Directories List*, which shows the subdirectories in the current directory. Select directories in descending order to move down a level.
- The *Files List*, which shows files in the current subdirectory.
- Buttons that let you open and delete files, delete directories, cancel any operation, and get Help.

The next step depends on whether you open an existing or new configuration file. Go to one of the following sections:

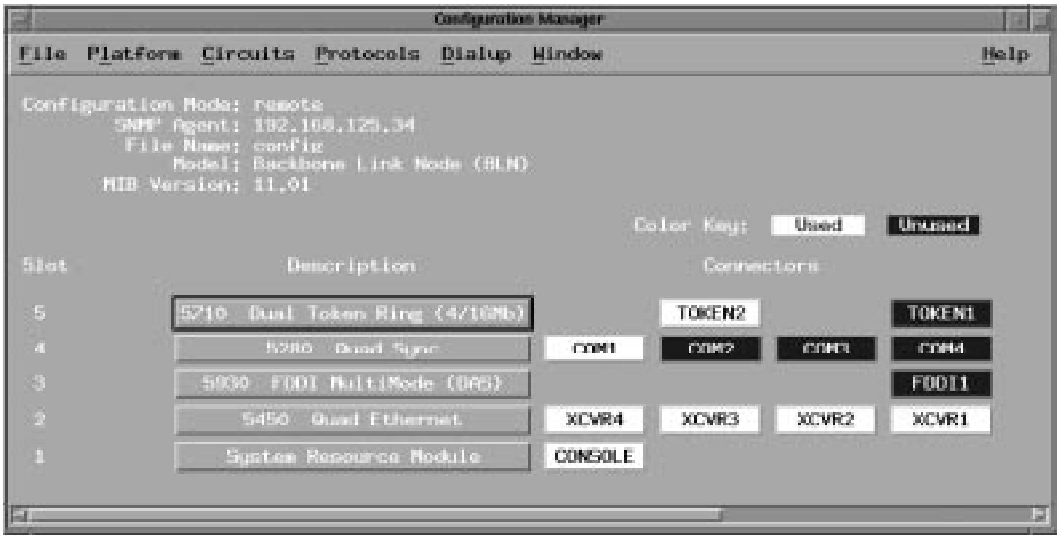
- Opening an Existing Configuration File on page 2-10
- Opening a New Configuration File on page 2-11

Opening an Existing Configuration File

To open an existing file, use one of the following methods:

- Click on the correct path by selecting options in the Path List, Directories List, and Files List boxes, then click on Open File.
- Enter the correct names in the Path, Directory, and Files fields, then click on Open File.

  After you open a file, the Configuration Manager opens and displays a logical image of the router's connectors. Figure 2-7 shows the connectors on a BLN®.



Configuration Mode: remote
SNMP Agent: 192.168.125.34
File Name: config
Model: Backbone Link Node (BLN)
MIB Version: 11.01

Color Key: Used Unused

Slot	Description	Connectors			
5	5710 Dual Token Ring (4/16Mb)		TOKEN2		TOKEN1
4	5280 Quad Sync	COM1	COM2	COM3	COM4
3	5930 FDDI MultiMode (DAS)				FDDI1
2	5456 Quad Ethernet	XCVR4	XCVR3	XCVR2	XCVR1
1	System Resource Module	CONSOLE			

Figure 2-7. Configuration Manager Window

For information about modifying a configuration file, go to Chapter 3.

Opening a New Configuration File

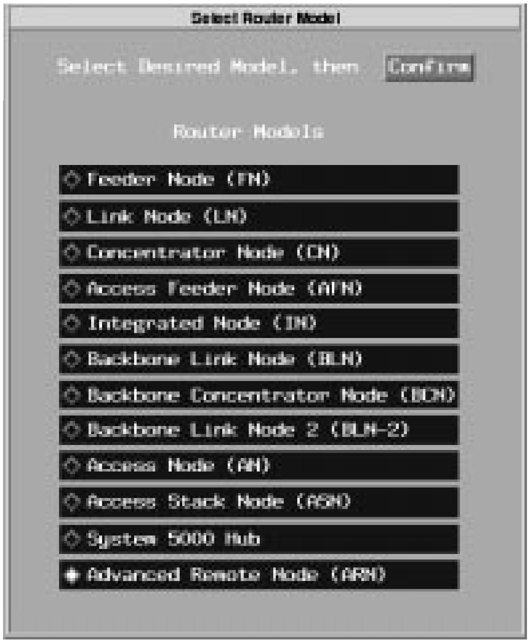
You must have write-access privileges to the directory where you want to create a configuration file.

To open a new configuration file:

1. **In the File Selection window, specify the file name (refer to Figure 2-6).**

    - Click on the correct path by selecting options in the Path List, Directories List, and Files List boxes, then click on Open File.
    - Enter the correct names in the Path, Directory, and Files fields, then click on Open File.

    The Select Router Model window opens, listing Bay Networks router models (Figure 2-8).



Select Router Model

Select Desired Model, then Confirm

Router Models

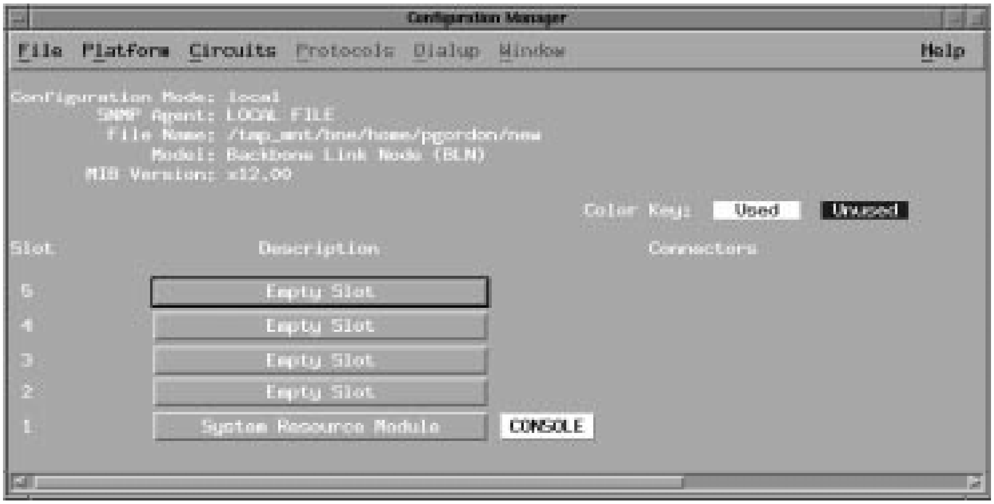
○ Feeder Node (FN)
○ Link Node (LN)
○ Concentrator Node (CN)
○ Access Feeder Node (AFN)
○ Integrated Node (IN)
○ Backbone Link Node (BLN)
○ Backbone Concentrator Node (BCN)
○ Backbone Link Node 2 (BLN-2)
○ Access Node (AN)
○ Access Stack Node (ASN)
○ System 5000 Hub
● Advanced Remote Node (ARN)

Figure 2-8. Select Router Model Window

2. **Select the appropriate router, and then click on Confirm.**

The Configuration Manager opens and displays the logical image of the router's connectors (Figure 2-9).

If you are configuring an ARN, go to "Opening a New Configuration File for an ARN Router" on page 2-14.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /tmp_mnt/bne/home/pgordon/new
             Model: Backbone Link Node (BLN)
       MIB Version: x12.00
```

Slot	Description	Connectors
5	Empty Slot	
4	Empty Slot	
3	Empty Slot	
2	Empty Slot	
1	System Resource Module	CONSOLE

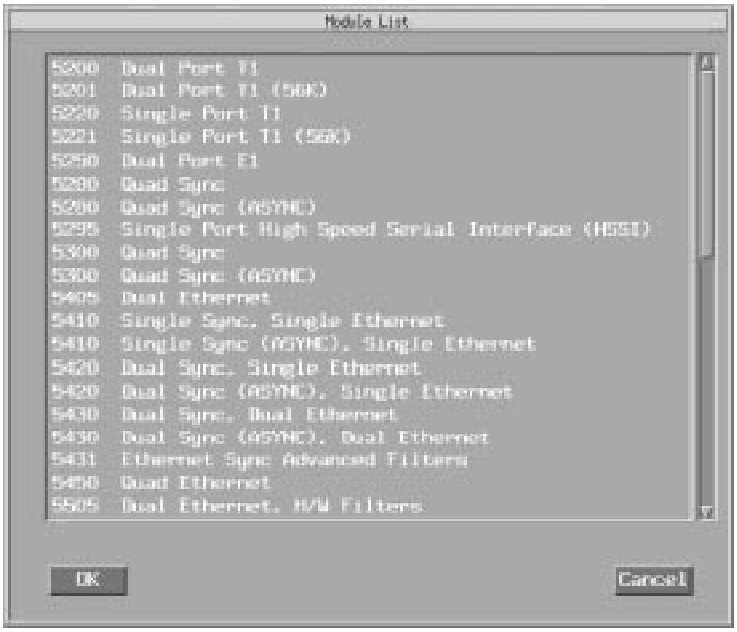
Figure 2-9. Configuration Manager Window for a New Configuration File

3. **Specify the router's hardware.**

   In local mode, the Configuration Manager requires that you specify the hardware configuration whenever you create a new configuration file. You can add hardware to empty slots and change the hardware in occupied slots. The procedure for both is the same.

   a. **Click on the box labeled Empty Slot to specify hardware for a slot.**

      The Module List window opens, which lists the modules and their corresponding model numbers (Figure 2-10).



```
5200  Dual Port T1
5201  Dual Port T1 (56K)
5220  Single Port T1
5221  Single Port T1 (56K)
5250  Dual Port E1
5280  Quad Sync
5280  Quad Sync (ASYNC)
5295  Single Port High Speed Serial Interface (HSSI)
5300  Quad Sync
5300  Quad Sync (ASYNC)
5405  Dual Ethernet
5410  Single Sync, Single Ethernet
5410  Single Sync (ASYNC), Single Ethernet
5420  Dual Sync, Single Ethernet
5420  Dual Sync (ASYNC), Single Ethernet
5430  Dual Sync, Dual Ethernet
5430  Dual Sync (ASYNC), Dual Ethernet
5431  Ethernet Sync Advanced Filters
5450  Quad Ethernet
5505  Dual Ethernet, H/W Filters
```

Figure 2-10. Module List Window

b. **Click on the hardware module you want for that slot.**

   Scroll through the window to see all the modules.

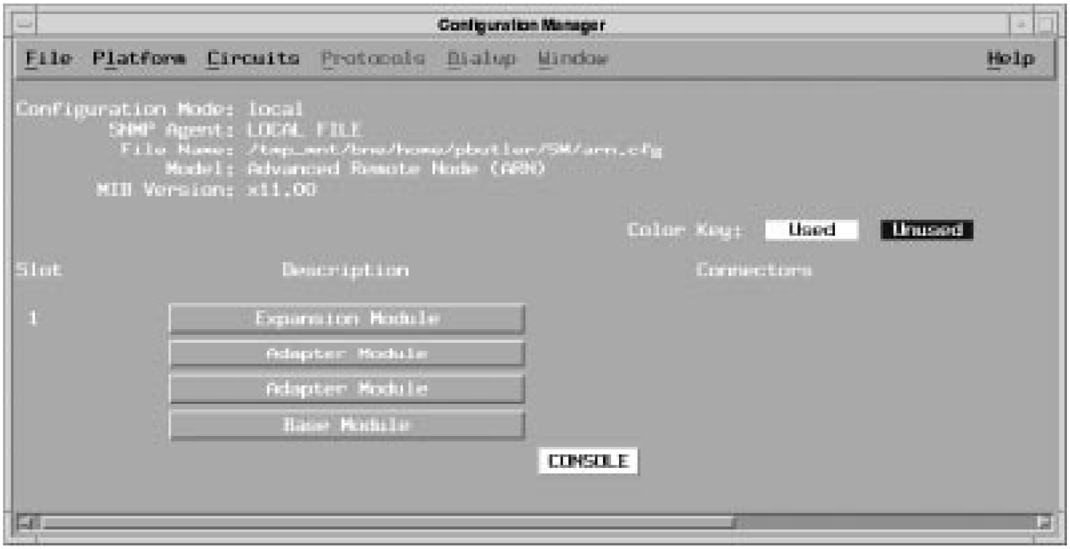
c. **Click on OK.**

You return to the Configuration Manager window, which now displays the slot with the module you selected.

4. **Specify modules for any other slots you want to configure.**
5. **Go to Chapter 3 to modify the configuration file.**

Opening a New Configuration File for an ARN Router

When you open a new configuration file for an ARN router, the Configuration Manager window displays the logical image of the ARN router's connectors (Figure 2-11).



Configuration Mode: local
SNMP Agent: LOCAL FILE
File Name: /tmp_mnt/bno/home/pbutler/SM/arn.cfg
Model: Advanced Remote Node (ARN)
MIB Version: x11.00

Figure 2-11. Configuration Manager Window for a New Configuration File (ARN)

1. **In the Configuration Manager window, click on Base Module.**

   The Module List window for the ARN opens (Figure 2-12).

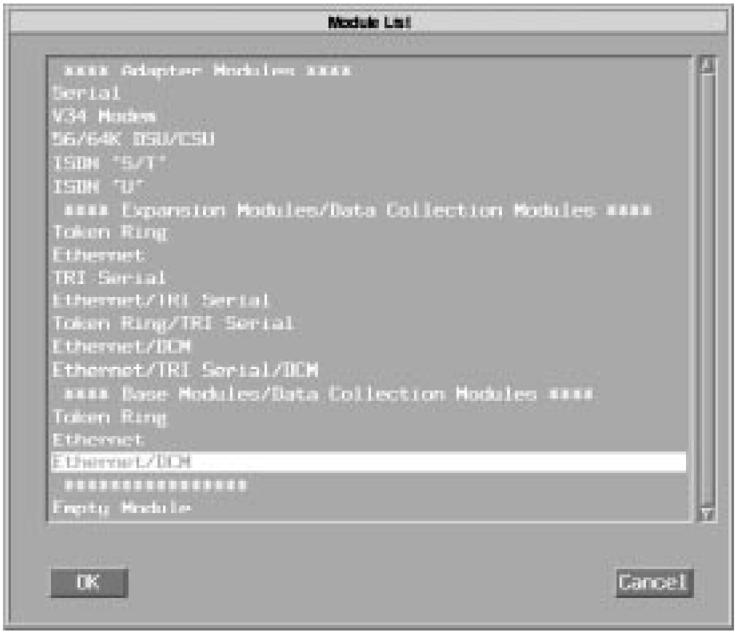


Figure 2-12. Module List Window for an ARN Base Module

2. **Select the base module configuration from the Base Modules/Data Collection Modules list.**

   If the ARN base module contains an installed RMON data collection module (DCM), select Ethernet/DCM.

3. **Click on OK.**

   You return to the Configuration Manager window, which now displays the interfaces for the base module selected.

4. **If the ARN contains no expansion or adapter modules, configure the base module interfaces next.**

5. **If the ARN contains only an expansion module, go to step 11.**

6. **If the ARN contains a WAN adapter module installed in a front panel slot, click on Adapter Module in the Configuration Manager window.**

   The Module List window opens (Figure 2-13).

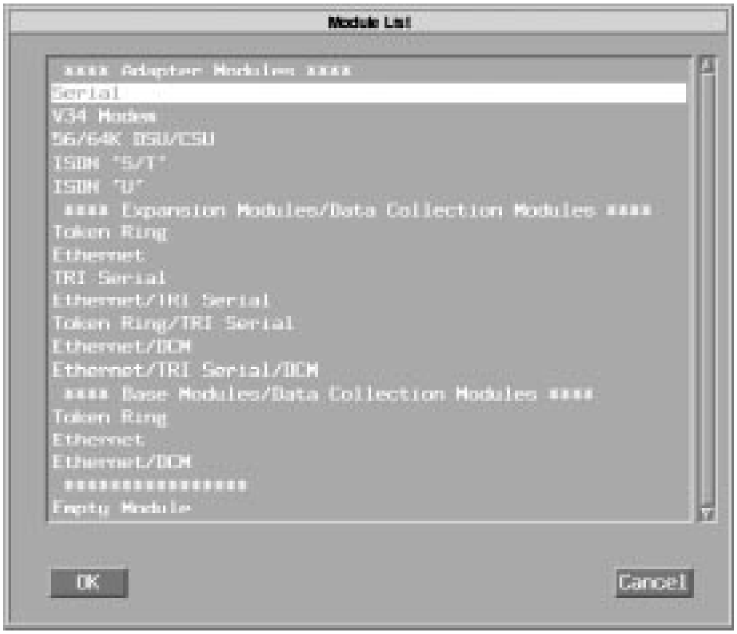


Figure 2-13. Module List Window for an ARN Adapter Module

7. **Select the WAN module type from the Adapter Modules list at the top of the window.**

   You return to the Configuration Manager window, which now displays an interface for the selected adapter module.

8. **To select a second WAN adapter module, repeat steps 6 and 7.**

9. **If the ARN contains no expansion module, configure the ARN module interfaces next.**

10. **Click on Expansion Module in the Configuration Manager window.**

    The Module List window opens (Figure 2-14).

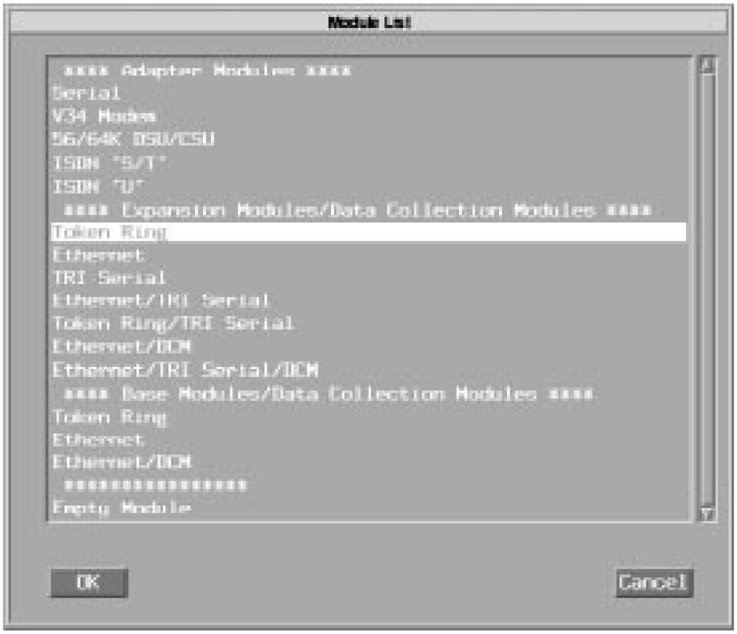
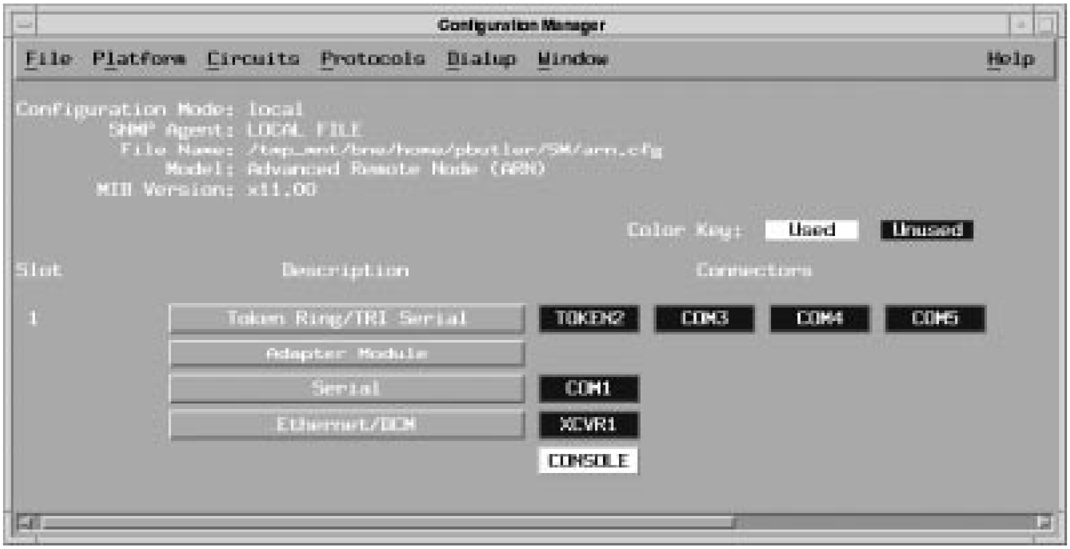


Figure 2-14. Module List Window for an ARN Expansion Module

11. **Select the expansion module type from the Expansion Modules/Data Collection Modules list.**

12. **Click on OK.**

    You return to the Configuration Manager window, which now displays the expansion module interfaces. Figure 2-15 shows the interfaces for a sample configuration.



Configuration Manager

```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /tmp_mnt/bnw/home/pbutler/SM/arn.cfg
             Model: Advanced Remote Node (ARN)
       MIB Version: x11.00
```

Slot	Description	Connectors			
1	Token Ring/TRI Serial	TOKEN2	COM3	COM4	COM5
	Adapter Module				
	Serial	COM1			
	Ethernet/DCM	XCVR1			
		CONSOLE			

Figure 2-15. Sample ARN Module Configuration

13. **Go to Chapter 3 to modify the configuration file.**

Remote Mode

Remote mode lets you access the router over the network and retrieve the configuration file from the router. You can then modify the configuration, save it, and implement it at a later time by rebooting the router. This mode allows you to change the router's configuration at a time that will least interrupt productivity.

In most situations, Bay Networks recommends using remote mode because you do not have to configure the hardware; the Configuration Manager reads the hardware automatically.

In remote mode, you do not need to manually transfer the configuration file to and from the router. Site Manager automatically retrieves the file from the router using TFTP, and automatically sends the file back to the router when you save it. Essentially, remote mode is similar to local mode with an automatic TFTP function when you open and subsequently save a configuration file.

If the file you open in remote mode has the same name as a local file on the Site Manager workstation, Site Manager asks whether you want to back up the local file. If you choose to save the local file, Site Manager then renames it to *<file_name>.bak*.

Opening a New or Existing Configuration File in Remote Mode

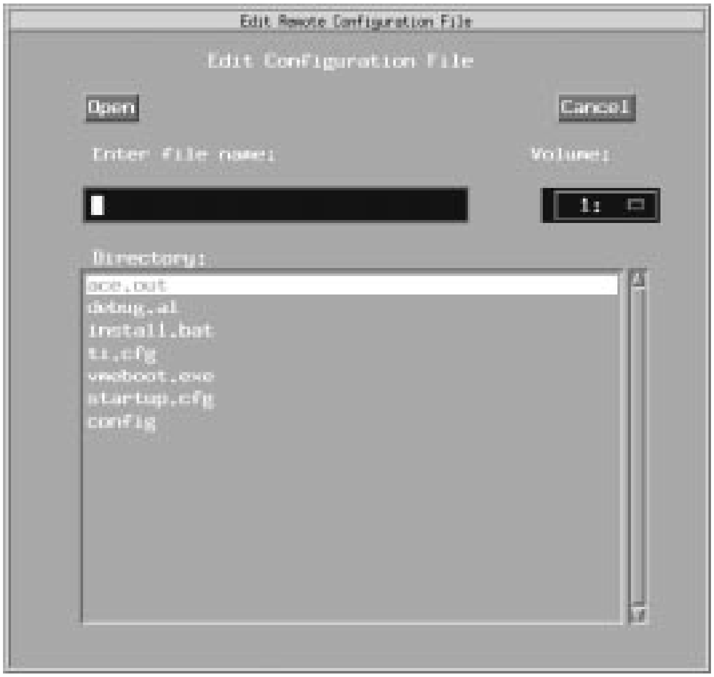
To open a configuration file in remote mode:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools** > **Configuration Manager** > **Remote File.**

   The Edit Remote Configuration File window opens (Figure 2-16).



Volume: 1:

Figure 2-16. Edit Remote Configuration File Window

3. **Retrieve a configuration file from the router as follows:**

   a. **In the Volume field, select a volume. This is the volume of an existing configuration file or the destination volume for a new file.**

      When you click in the Volume field, a menu listing the volumes opens. When you select a volume, its contents are displayed in the Directory list.

   b. **Specify a file name in the Enter file name field.**

      Type a new file name or select a file name from the Directory list.

   c. **Click on Open.**

If you selected an existing file, the Configuration Manager retrieves the file and displays the router's connectors (refer to Figure 2-7); the file name appears in the upper left corner of the main Configuration Manager window.

4. **Go to Chapter 3 to modify the configuration file.**

Dynamic Mode

Dynamic mode lets you access the router over the network and configure the router in real time. Any changes you make happen immediately in RAM, but they are not written to flash memory (or diskette on older routers) until you save the file.

Do not use dynamic mode to create an entirely new router configuration file. Instead, use it to make minor changes to an existing configuration file. It is safer to create a configuration file using local or remote mode, because it is easier to correct mistakes or redo a configuration.

Also, configuring a router in dynamic mode can interrupt service, depending on the attributes you modify. Be careful when modifying the global attributes of protocols. For example, changing the size of the bridge forwarding table will flush and re-create the table, which can briefly affect performance.

Opening a Configuration File in Dynamic Mode

To open a configuration file in dynamic mode:

1. **In the main Site Manager window, connect to a router you want to configure.**

   Refer to Chapter 1 for instructions.

2. **Choose Tools** > **Configuration Manager** > **Dynamic.**

   If you used the Technician Interface to set the router to secure mode during the Quick-Start procedure, you will be prompted for a password when you try to change a parameter value. Enter the encryption key that you used when you set this router to secure mode.

   The Configuration Manager window opens, displaying the real-time router hardware and software configuration.

➡ **Note:** You will need to save the configuration file in dynamic mode for the router to update the file’s MIB stamp to match the newer software.

3. **Go to Chapter 3 to modify the configuration file.**

The Configuration Manager and the Technician Interface

The Technician Interface is a command-line interface that provides management access to a Bay Networks router. Using the Technician Interface, you can configure some parameters, disable or enable protocols, and monitor router operation. For more information, refer to *Using Technician Interface Software*.

One way to access the Technician Interface is through a direct or dial connection to the router's console port.

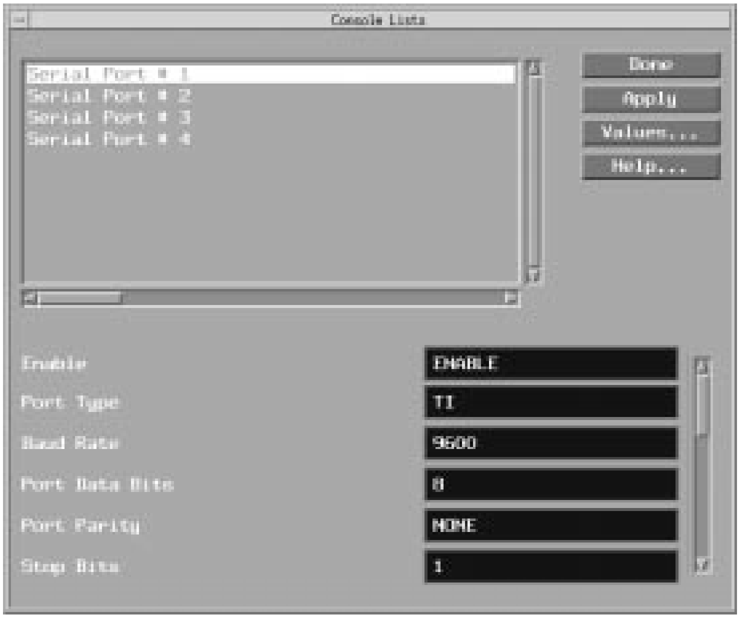
To configure the console port to access the Technician Interface:

1. **In the main Site Manager window, choose Tools > Configuration Manager > Local File/Remote File/Dynamic.**

   The Configuration Manager window opens (refer to Figure 2-7).

2. **Click on Console.**

   The Console Lists window opens (Figure 2-17).



Enable ENABLE
Port Type TI
Baud Rate 9600
Port Data Bits 8
Port Parity NONE
Stop Bits 1

Figure 2-17. Console Lists Window

The Console Lists window displays the router’s console (serial) ports. Console ports are the physical ports on a router for system input and output. The number of ports depends on the router model.

3. **Select a console port from the Console Lists window.**
4. **Edit the parameters.**

   Refer to the parameter descriptions beginning on page B-5 or click on Help.
5. **Click on Apply to save your changes.**
6. **Click on Done after you configure all the ports.**

   You return to the Configuration Manager window.

Customizing the ARN V.34 Console Modem Port

In addition to the console port, the ARN supports an integrated V.34 modem to access the Technician Interface.

➡ **Note:** When the V.34 console modem port is installed in the ARN, the default console modem port is disabled.

Refer to *Installing and Operating BayStack ARN Routers* for information about cabling a service console device and configuring a serial terminal or modem.

The integrated V.34 modem is set to operate as a remote console using a factory-default configuration. Bay Networks recommends using this default configuration.

The modem defaults are set by the following factory-default AT command initialization string:

```
ATT&d0&k4&X0S0=2S2=43
```

Table 2-1 on page 2-24 lists the default settings for the V.34 console modem.

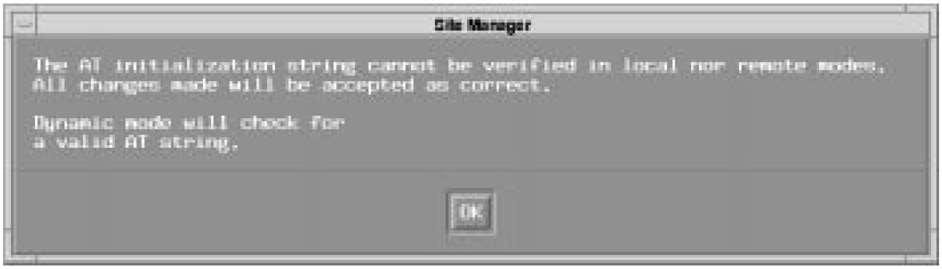
Table 2-1. ARN V.34 Console Modem Defaults

Modem Signal/Parameter	Value
Clear To Send (CTS)	On
Data Terminal Ready (DTR)	Set to answer all incoming calls.
Data Carrier Detect (DCD) or RLSD	On while carrier is present. (The ARN uses DCD to detect modem connect and disconnect.)
Data Set Ready (DSR)	On
Ready to Send (RTS)	Ignored
Synchronous/Asynchronous Mode	Asynchronous
AutoAnswer	Answer on two rings with DTR active.
Local Character Echo	Off
Supervisory Functions	Off
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None

To change the default modem initialization string for an ARN V.34 console modem port:

1. **In the Configuration Manager window, choose Platform > V34 Modem.**

   The Configuration Manager displays the following warning message about editing the AT modem initialization string.

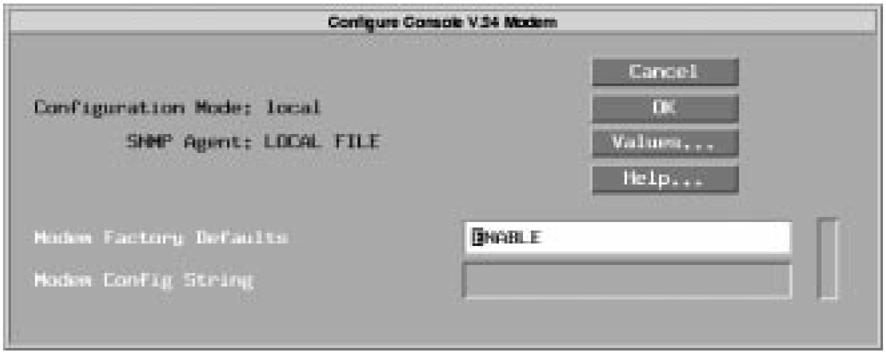


The AT initialization string cannot be verified in local nor remote modes.
All changes made will be accepted as correct.

Dynamic mode will check for
a valid AT string.

2. **Read the message and click on OK.**

   The Configure Console V.34 Modem window opens (Figure 2-18).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Modem Factory Defaults ENABLE
Modem Config String

Figure 2-18. Configure Console V.34 Modem Window

3. **Set the Modem Factory Defaults parameter to Disable.**

   Click on Help for parameter descriptions.

4. **In the Modem Config String parameter, enter a standard AT command string.**

Caution: Entering an invalid command string could disable the modem. Site Manager can verify AT command string changes only when in dynamic mode.

Refer to *Configuring Dial Services* for a summary of AT modem initialization commands for the ARN.

5. **Click on OK.**

Chapter 3
Modifying and Saving Router Configurations

This chapter describes how to use the Configuration Manager to add and modify network interfaces. Most parameters are set to a default value that is suitable for most networks; however, the Configuration Manager lets you customize these settings.

Bay Networks provides documentation that contains information and instructions for configuring network interfaces for a particular protocol. After you are familiar with the configuration process, documented in this chapter, refer to the protocol-specific guides as necessary. See About this Guide for information about ordering any Bay Networks guide.

This chapter contains the following information:

Modifying a Router’s Configuration

If you are configuring a new router, you need to modify the initial configuration file, *startup.cfg*, which you created using the Quick-Start procedure. (For information about the Quick-Start procedure, refer to *Quick-Starting Routers*.)

If you are configuring a router that is already in your network, you need to modify an existing configuration file, usually named *config* (*config* is the default configuration file).

You can generate a report of the router’s configuration using the Report Generator. The Report Generator is useful because it converts the binary configuration file to ASCII format for easy reading, so that you can verify the configuration and troubleshoot any problems. Refer to Chapter 9 for information about the Report Generator.

For information about how to enter data in Configuration Manager windows, refer to Chapter 2.

Configuration Procedure

Table 3-1 outlines the configuration procedure for new and existing routers. This procedure provides maximum safety when altering a router’s configuration.

Local and remote configuration modes are the safest modes to work in; however, you can use any mode that suits your situation. For critical applications, when you must alter how the router is operating, use dynamic mode.

Bay Networks recommends that you always have a *config* file that you know works and test any new or modified configuration file under a unique name, for example, *test.cfg*. In this way, if the router has a problem starting, you can reset it and it will restart with the default file, *config* (refer to Chapter 4 for instructions about resetting the router).

This procedure is recommended for new and existing routers. In the case of a new router, although the *config* file does not represent a complete working configuration, you do not want to corrupt the *config* file. If the router should behave unpredictably, it is easier to recover with the *config* file.

Specific instructions for each task in Table 3-1 are located in this and other chapters. You may want to print or copy this procedure and use it as a checklist as you complete each task.

Table 3-1. Tasks to Configure a New or Existing Router

Task	Instructions
1. Connect to the router.	Refer to Chapter 1.
2. Verify free space on the destination router volume and, if applicable, compact flash memory.	Refer to “Verifying Available Space on the Destination Volume” on page 3-5.
3. Make a copy of the configuration file using the Router Files Manager. • For new routers, make a copy of *startup.cfg.* • For existing routers, make a copy of *config.*	Refer to “Making a Copy of the Existing Configuration File” on page 3-7.
4. Open a new file or the existing configuration file in any Configuration Manager mode. If you are using an existing file in local mode, you must manually transfer the configuration file to the Site Manager workstation before opening it.	Refer to Chapter 2.
5. Specify the router’s hardware for a new file (local mode only).	Refer to Chapter 2.
6. Modify the configuration file. For example, add a protocol interface or change parameter values.	Refer to “Configuring a Circuit” on page 3-12. For instructions on configuring a specific protocol, refer to the guide for that protocol.
7. Save the configuration file under a new name, for example, *test.cfg*.	Refer to “Saving Configuration Files” on page 3-30.
8. Transfer the configuration file to the router (local mode only).	Refer to “Saving a Configuration File in Local Mode” on page 3-30.
9. Perform a named boot to boot the router with the modified configuration file. This tests the new file before you rename it to *config*.	Refer to Chapter 4.
10. Rename the new configuration file to *config* after the router boots successfully. The new file is now the default *config* file.	Refer to Chapter 4.

Modifying Network Interfaces

Before you modify a configuration file, you should be familiar with the Configuration Manager's three operating modes and you should make sure that the Configuration Manager is operating on your UNIX workstation or PC. (Refer to Chapter 2 for information.)

You can add a protocol interface to the router, for example, a multiple IP interface, a WAN interface, or a LAN interface. After you add an interface to a router, you can use the Configuration Manager to customize it.

The Configuration Manager provides access to all parameters associated with an interface. These parameters consist of the physical layer (line) parameters, data link layer parameters, and network layer parameters. You can perform the following modifications:

- Modify the line parameters associated with the interface.

  Configuring WAN Line Services and *Configuring Ethernet, FDDI, and Token Ring Services* describe how to edit line parameters.

- Add and delete protocols from the circuit associated with the interface.
- Edit bridging and routing protocol parameters.

  You can access these parameters on a system-wide or interface-specific basis. Refer to the appropriate protocol-specific guide for instructions.

- Delete and rename circuits, as well as move a circuit to another interface.
- Add multiple IP addresses to a single circuit that supports IP.

Preparing to Modify a Configuration File

Before modifying a configuration file, you need to make sure that you do not corrupt any existing configuration file. The following sections tell you how to prepare for modifying an interface. (Chapter 5 provides additional detail about these procedures.)

Verifying Available Space on the Destination Volume

Before you save a configuration file in local or remote mode and reboot the router with it, make sure that the router's destination volume has enough space available for the file. If there is not enough space, you will have to copy the original files to another system and then delete them from the router.

To free up space on nonvolatile file systems (NVFS), that is, routers that use flash memory, you may need to compact the files. Before you compact memory, Bay Networks recommends that you back up the files by copying them to a second flash card. If possible, compact file space at off-peak times, because compacting a file uses up memory resources.

In addition to checking the space, look at the names of the existing configuration files to ensure that you save the new file under a unique name. Even if you change the name of the file to the default configuration file, *config*, you should initially test the file under a unique name.

Use the Router Files Manager to show the available and contiguous free space on the router as well as the files on the volume (refer to Chapter 5). Note that for routers that use flash memory, the volume is represented by the slot number of the flash media. For routers that use diskettes, the volume is indicated by the disk drive letter.

To start the Router Files Manager:

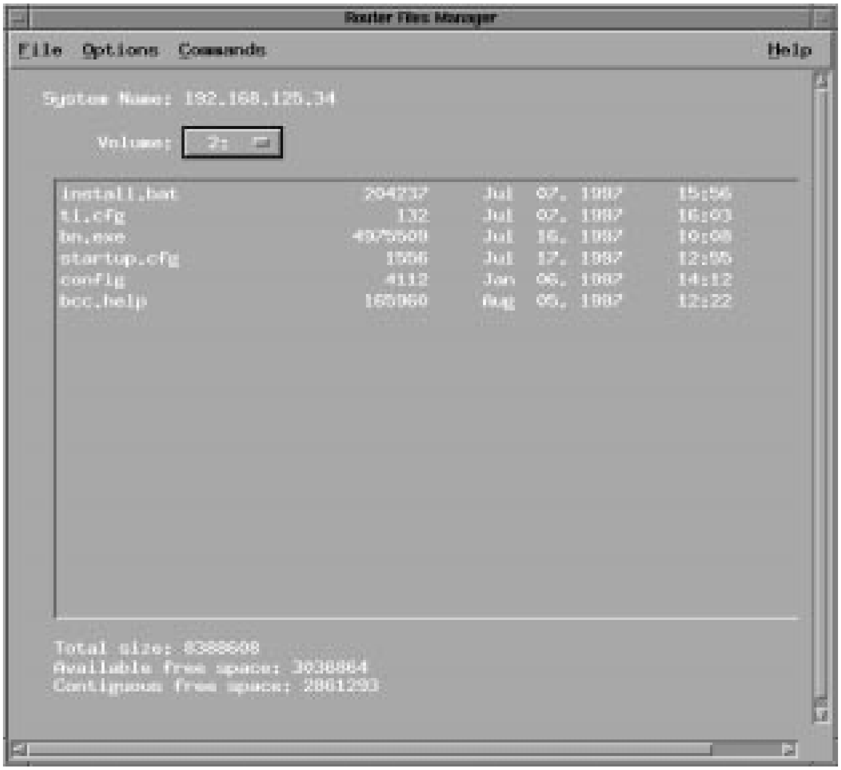
1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (Figure 3-1).

   This window lists the files, file sizes, and available free space.



```
System Name: 192.168.125.34

      Volume: 2:

install.bat           204237    Jul  07, 1997    15:56
ti.cfg                   132    Jul  07, 1997    16:03
bn.exe               4975508    Jul  16, 1997    10:08
startup.cfg             1556    Jul  17, 1997    12:55
config                  4112    Jan  06, 1997    14:12
bcc.help              165060    Aug  05, 1997    12:22

Total size: 8388608
Available free space: 3038864
Contiguous free space: 2861293
```

Figure 3-1. Router Files Manager Window

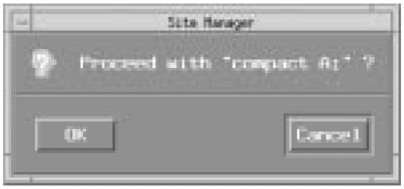
3. **Check the amount of free space.**

   -- For NVFS routers, that is, routers with flash memory, check the number of bytes displayed for contiguous free space.

   -- For DOS routers, that is, routers that use diskettes, check the number of bytes displayed for available free space.

4. **For flash memory cards only, choose Commands** > **Compact.**

   A confirmation window opens asking if you want to compact the files (Figure 3-2). Compacting the flash memory card optimizes the available space.



Proceed with "compact A:" ?

Figure 3-2. Compact Confirmation Window

5. **Click on OK.**

   You return to the Router Files Manager window (refer to Figure 3-1).

Caution: On AN and ANH routers, compacting memory can take up to 12 minutes. Do not reset the router during this time because you will corrupt the flash memory. Consequently, you will need to replace the flash memory to boot the router.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

Making a Copy of the Existing Configuration File

If you are configuring a new router, make a copy of *startup.cfg* and modify the copy. If you are configuring an existing router, make a copy of the *config* file.

To create a copy of a configuration file as a backup:

1. **Connect to the router.**

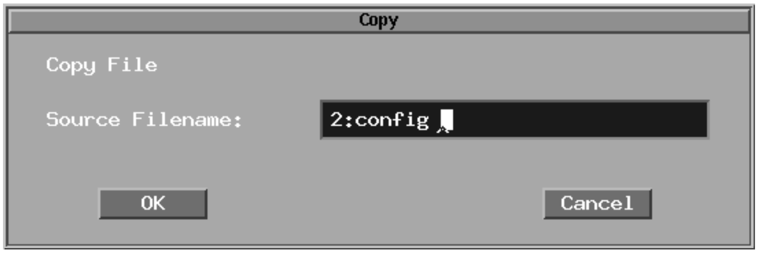
   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 3-1).

3. **Choose the router volume where the configuration file resides.**
4. **Choose the configuration file from the list of files.**
5. **Choose Commands > Copy.**

   The Copy window opens (Figure 3-3).



Copy

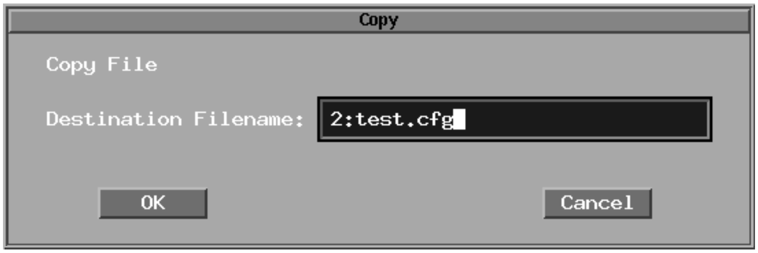
Copy File

Source Filename: 2:config

Figure 3-3. Copy Window (Source File Name)

6. **Type a source file name, then click on OK.**

   A second Copy window prompts you for the destination file name (Figure 3-4).



Copy

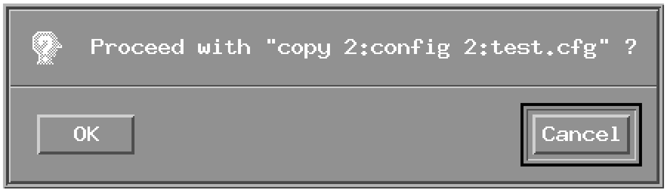
Copy File

Destination Filename: 2:test.cfg

Figure 3-4. Copy Window (Destination File Name)

7. **Type a new name for the file copy, in the format <*volume*><*filename*>, for example, *2:test.cfg*, then click on OK.**

   A confirmation window opens (Figure 3-5).



Proceed with "copy 2:config 2:test.cfg" ?

Figure 3-5. Copy Confirmation Window

8. **Click on OK.**

   The Router Files Manager copies the source file to the file name and volume you specified.

9. **Go to “Transferring the Configuration File to the Site Manager Workstation.”**

Transferring the Configuration File to the Site Manager Workstation

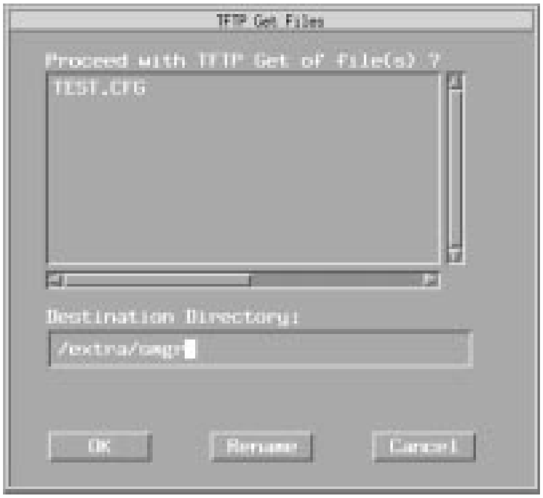
To transfer the copy of the configuration file from the router to your Site Manager workstation:

1. **In the Router Files Manager window, choose the router volume where you stored the copy of the file.**

2. **Choose the copied file.**

3. **Choose File > TFTP > Get File(s).**

   The TFTP Get Files window opens (Figure 3-6).



Proceed with TFTP Get of File(s) ?

TEST.CFG

Destination Directory:

/extra/smgr

Figure 3-6. TFTP Get Files Window

4. **In the Destination Directory field, type the directory where you want to store the file on your Site Manager workstation.**

5. **Click on OK.**

   The configuration file now resides in a directory on your Site Manager workstation.

   You return to the Router Files Manager.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

Adding a Circuit to an Interface

The Configuration Manager simplifies router configuration by providing default values for most of the parameters required to configure an interface. To customize the configuration for your network, you can modify these parameter defaults.

To add a network interface, you must configure a circuit then enable bridging or routing protocols for that circuit. The next section details these procedures.

Circuit Naming Conventions

When you configure a circuit on an interface, you assign the circuit a name. Initially, Site Manager provides a circuit name, which, for most routers, consists of a letter that indicates the circuit type followed by two numbers that identify the circuit location. The first number is from 1 to 14 and identifies the router slot. The second number is from 1 to 8 and identifies the specific connector in that slot. For example, the circuit name S51 identifies a synchronous circuit in slot 5 on communications port 1.

Circuit names for the ASN router differ. The name consists of a letter indicating the circuit type, followed by three numbers which identify the ASN in the stack and the circuit location. The first number is the slot ID of the ASN router in the stack, which Site Manager refers to as the slot. The second number is the net module, and the third number is the connector. For example, the circuit name E321 identifies an Ethernet circuit on port 1 of the second net module for the third ASN in the stack.

Table 3-2 on page 3-12 lists the circuit-type letter and its meaning.

Table 3-2. Understanding Letters in Circuit Names

Circuit-Type Letter	Connector Type
E	Ethernet
E1	E1
F	FDDI
H	HSSI
MCE1	MCE1
MCT1	MCT1
O	Token ring
S	Synchronous
T1	T1

Use the circuit-naming convention to consistently name circuit types and locations. You can, however, assign any circuit name containing up to 15 characters (alphanumeric, underline, or slash) without spaces. Circuit names are case-sensitive.

Configuring a Circuit

To configure a circuit:

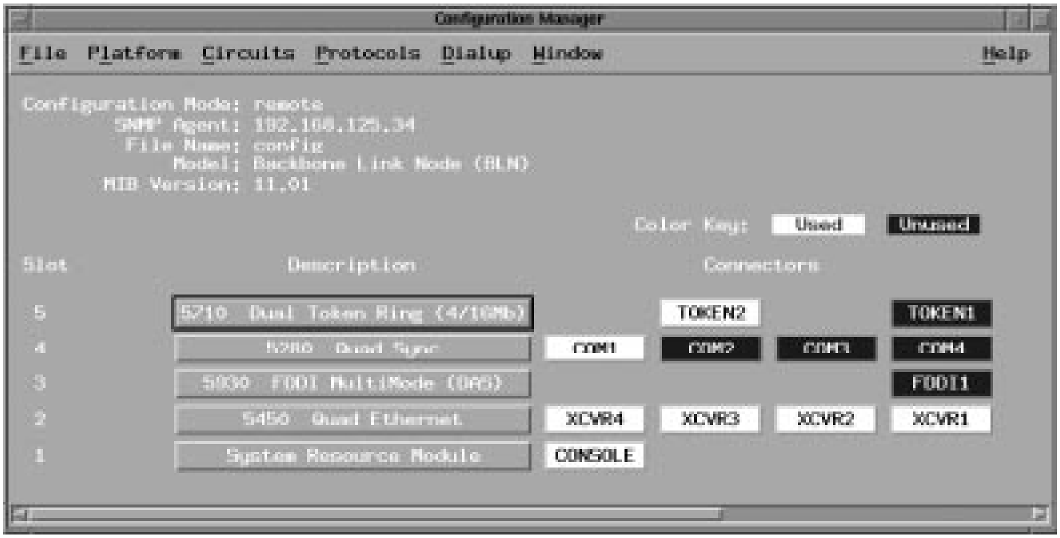
1. **In the main Site Manager window, choose Tools > Configuration Manager > Local File/Remote File/Dynamic.**

2. **Open the file that you just transferred or a new file.**

   If you are opening an existing file in local or remote mode, you must open the file before Site Manager displays the Configuration Manager window.

   If you are opening a new file in local mode, you have to select the router platform and the hardware before Site Manager displays the Configuration Manager window.

   The Configuration Manager window opens (Figure 3-7).



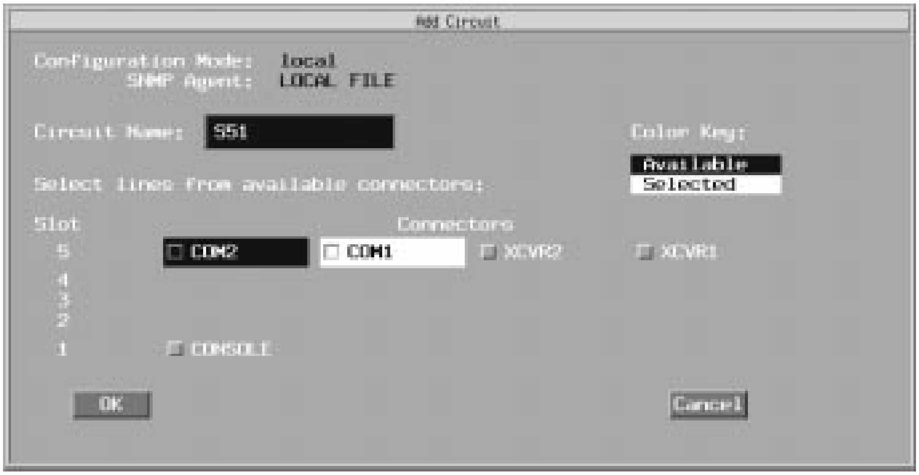
```
Configuration Mode: remote
        SNMP Agent: 192.168.125.34
         File Name: config
             Model: Backbone Link Node (BLN)
       MIB Version: 11.01
```

Slot	Description	Connectors			
5	5710 Dual Token Ring (4/16Mb)		TOKEN2		TOKEN1
4	5280 Quad Sync	COM1	COM2	COM3	COM4
3	5930 FDDI MultiMode (DAS)				FDDI1
2	5450 Quad Ethernet	XCVR4	XCVR3	XCVR2	XCVR1
1	System Resource Module	CONSOLE			

Figure 3-7. Configuration Manager Window

3. **Click on the connector for the network interface.**

   The Add Circuit window opens (Figure 3-8).



```
Configuration Mode:  local
        SNMP Agent:  LOCAL FILE

Circuit Name: S51

Select lines from available connectors:
```

Slot	Connectors			
5	□ COM2	□ COM1	□ XCVR2	□ XCVR1
4				
3				
2				
1	□ CONSOLE			

Figure 3-8. Add Circuit Window

Except for MCT1 and MCE1 connectors, the Configuration Manager automatically sets all physical layer parameters, that is, the line parameters, to default values for the type of connector you select. For all LAN connections, the Configuration Manager also configures the data link layer connection for the LAN circuit.

4. **Accept the default circuit name or type a new one, then click on OK.**

   Refer to "Circuit Naming Conventions" on page 3-11 for information about naming conventions.

5. **If the connector supports hardware filters, a window prompts:**

   ```
   Do you want to enable Hardware Filters on this circuit?
   ```

   Click on OK to enable hardware filters. Otherwise, click on Cancel to exit the window. You return to the Add Circuit window.

6. **Click on OK.**

7. **Go to the next section to add protocols.**

Adding a Protocol to a Circuit

After you name a circuit, the Configuration Manager opens a LAN or WAN protocols menu, depending on the type of circuit you are configuring. After you enable a protocol on a circuit, you have configured a network interface.

Go to one of the following sections to enable a protocol:

- "Configuring a LAN Protocol for a Circuit," next in this chapter.

  Refer to this section if you configured any LAN circuits, for example, Ethernet, FDDI, or token ring.

- "Configuring a WAN Protocol for a Circuit" on page 3-16

  Refer to this section if you configured any WAN circuits, for example, COM, MCT1, or ISDN circuits.

Configuring a LAN Protocol for a Circuit

After you add a LAN circuit, the Select Protocols window opens (Figure 3-9).

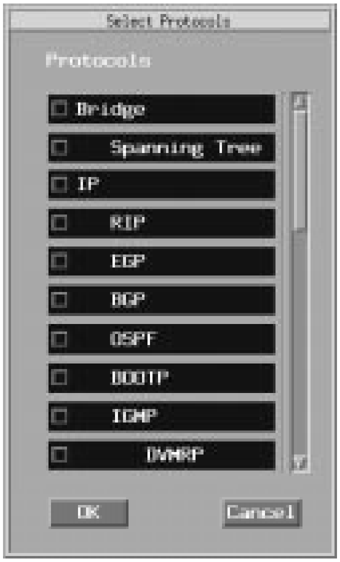


Figure 3-9. Select Protocols Window

The Select Protocols window varies according to circuit type, displaying only those protocols that the circuit type supports. In addition, for certain circuit types, the window allows you to select the protocol prioritization feature (refer to *Configuring Traffic Filters and Protocol Prioritization* for instructions).

To select bridging or routing protocols for a circuit:

1. **Click on the box to the left of the protocols you want to enable, then click on OK.**

   In some cases, the Configuration Manager opens a protocol-specific configuration window prompting for additional information. You cannot enable the protocol unless you configure these parameters. For information about specific protocol parameters, refer to the protocol-specific documentation. Any parameter that does not require information uses the default value.

   Some protocols (for example, Bridge, VINES, and NetBIOS) require no additional information to provide default service.

If you select a protocol service, that protocol is enabled. For example, if you select RIP or OSPF, the Configuration Manager enables IP because RIP and OSPF are services of IP.

2. **Specify the required information in each protocol-specific window that opens.**

3. **Click on OK.**

   After you define all protocols for the circuit, you return to the Configuration Manager window. The connector is highlighted to indicate that the interface is configured.

   The Configuration Manager then opens the window for the next protocol enabled on the circuit.

Configuring a WAN Protocol for a Circuit

After you add a WAN circuit, the WAN Protocols window opens (Figure 3-10).

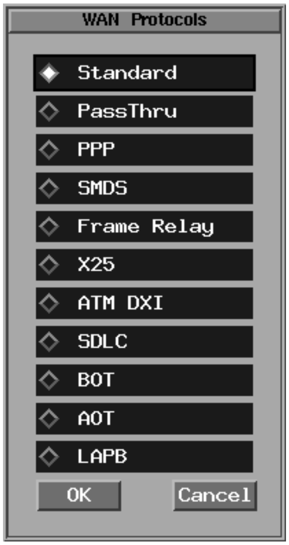


Figure 3-10. WAN Protocols Window

To select WAN protocols for a circuit:

1. **Click on the box to the left of the protocols you want to enable, then click on OK.**

   When you select a WAN protocol, note the following:

   - Selecting frame relay, PPP, or SMDS automatically enables protocol prioritization. For information about protocol prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization.*
   - If you select Bay Networks Standard protocol, you cannot change the WAN protocol on this circuit to any other protocol. If you want to enable another protocol on this circuit, you must delete the circuit and create a new one. For instructions on deleting a circuit from the router, refer to "Deleting a Circuit from the Router" on page 3-26.
   - When you enable a WAN protocol, the synchronous line parameters are automatically set to the following values.

Parameter	Setting
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	WAN protocol you enabled

     Refer to *Configuring WAN Line Services* for more information.
   - If you are configuring the COM2 port on an AN or ANH router, the Edit ASYNC Parameters window opens. See *Configuring WAN Line Services* for information about this window.

2. **After you choose a WAN protocol, do one of the following:**

   - Select a LAN protocol for this circuit, if prompted by the Configuration Manager.

     For some WAN protocols, such as Bay Networks Standard, PassThru, PPP, and frame relay, the Configuration Manager displays the Select Protocols window (refer to Figure 3-9), prompting you to select a LAN protocol. Depending on the protocol you choose, you may need to configure a few parameters. Refer to the protocol-specific documentation for configuration instructions.

- Specify values for WAN configuration parameters, if prompted by the Configuration Manager.

  For some WAN protocols, such as ATM DXI, SMDS, SDLC, and X.25, you must configure certain parameters immediately after selecting the WAN protocol for a circuit. Refer to the appropriate WAN documentation for instructions on configuring protocol parameters.

After you define all protocols for the circuit, you return to the Configuration Manager window. The connector is highlighted to indicate that the interface has been configured.

After you add a network interface you can:

- Add more network interfaces (repeat the previous procedures).
- Modify existing network interface (refer to “Modifying Circuits on an Interface” on page 3-19).
- Save and implement your new configuration file (refer to “Saving Configuration Files” on page 3-30).

Modifying Circuits on an Interface

You can modify existing circuits in the following ways:

- Add protocols to a circuit.
- Move a circuit.
- Rename a circuit.
- Assign additional IP addresses to a circuit.
- Delete protocols from a circuit.
- Delete a circuit from the router.

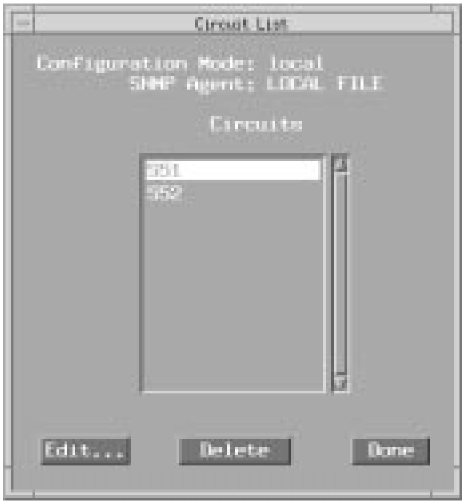
The sections that follow explain how to do these tasks.

Adding Protocols to a Circuit

To add protocols to an existing circuit:

1. **In the Configuration Manager window, choose Circuits** > **Edit Circuits.**

   The Circuit List window opens (Figure 3-11).



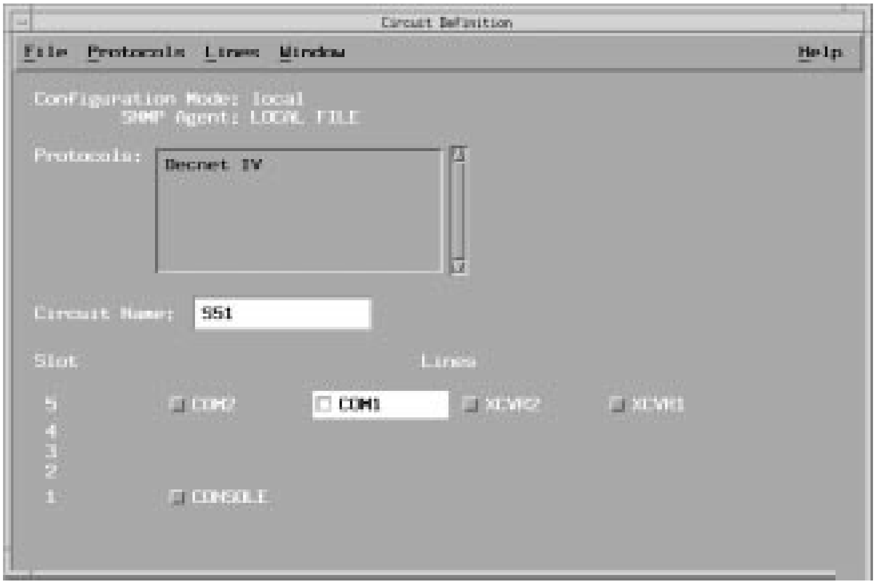
Configuration Mode: local
SNMP Agent: LOCAL FILE

Figure 3-11. Circuit List Window

2. **Choose the circuit to which you want to add protocols.**

3. **Click on Edit.**

   The Circuit Definition window opens (Figure 3-12).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Protocols: Decnet IV

Circuit Name: 551

Figure 3-12. Circuit Definition Window

4. **Choose Protocols** > **Add/Delete.**

   The Select Protocols window opens (refer to Figure 3-9).

5. **Choose the protocols that you want add to this circuit; then click on OK.**

   For each protocol you add, the Configuration Manager displays a protocol-specific configuration window.

6. **Configure each protocol you are adding.**

   Refer to the appropriate protocol-specific documentation.You return to the Circuit Definition window when the protocol configuration is complete.

7. **Repeat steps 1 through 6 for each circuit requiring additional protocols.**

8. **Choose File** > **Exit.**

   You return to the Circuit List window.

9. **Click on Done.**

Moving a Circuit

After you configure a circuit on a network interface, you can move the circuit to another interface. Moving a circuit is useful if you plan to replace a hardware module and you do not want to lose a configured interface.

When you move a circuit to a different type of network interface, for example, from an Ethernet interface to an FDDI interface, the Configuration Manager accounts for the changes in the physical layer configuration and automatically adjusts the line detail parameters accordingly.

To move a circuit:

1. **In the Configuration Manager window, choose Circuits > Edit Circuit.**

   The Circuit List window opens (refer to Figure 3-11).

2. **Choose the circuit that you want to move.**
3. **Click on Edit.**

   The Circuit Definition window opens with the name of the selected circuit in the Circuit Name field and the connector for the circuit interface highlighted (refer to Figure 3-12).

4. **Click on the circuit's connector.**

   The Configuration Manager removes the circuit from the connector, and the connector is no longer highlighted.

5. **Click on the new connector for the circuit interface.**

   The connector you chose is now highlighted, indicating that the circuit now connects to it.

   You may want to rename the circuit if you think the old circuit name may cause confusion. To do this, enter a new name in the Circuit Name field.

6. **Choose Lines > Change Lines.**

   You return to the Circuit Definition window, which reflects all circuits that have moved.

7. **Repeat steps 1 through 6 for each circuit that you want to move.**
8. **Choose File > Exit.**

   You return to the Circuit List window.

9. **Click on Done.**

Renaming a Circuit

You may want to rename a circuit if you moved the circuit from one interface to another. The circuit name reflects the location of the connector and if it is moved, the old name may cause confusion.

To rename a circuit on the router:

1. **In the Configuration Manager window, choose Circuits** > **Edit Circuits.**

   The Circuit List window opens (refer to Figure 3-11).

2. **Chose the circuit that you want to rename.**
3. **Click on Edit.**

   The Circuit Definition window opens (refer to Figure 3-12).

4. **Type a new name for this circuit in the Circuit Name box.**
5. **Choose Lines** > **Change Lines.**

   The Circuit Definition window reflects the change.

6. **Repeat steps 1 through 5 for each circuit that you want to rename.**
7. **Choose File** > **Exit.**

   You return to the Circuit List window.

8. **Click on Done.**

Assigning an Additional IP Address to a Circuit

Bay Networks IP routing supports multinet, which lets you assign multiple IP addresses to a single circuit. With multinet, a single circuit supports multiple IP network interfaces. Use multinet if you want to subnet a Class C address. Each IP address on a multinet circuit must belong to a unique network and subnet. You cannot have two interfaces for the same subnet. You can assign any number of IP addresses to a circuit. For more information about multinet, see *Configuring IP Services*.

To assign additional IP addresses to a circuit:

1. **In the Configuration Manager window, choose Circuits > Edit Circuits.**

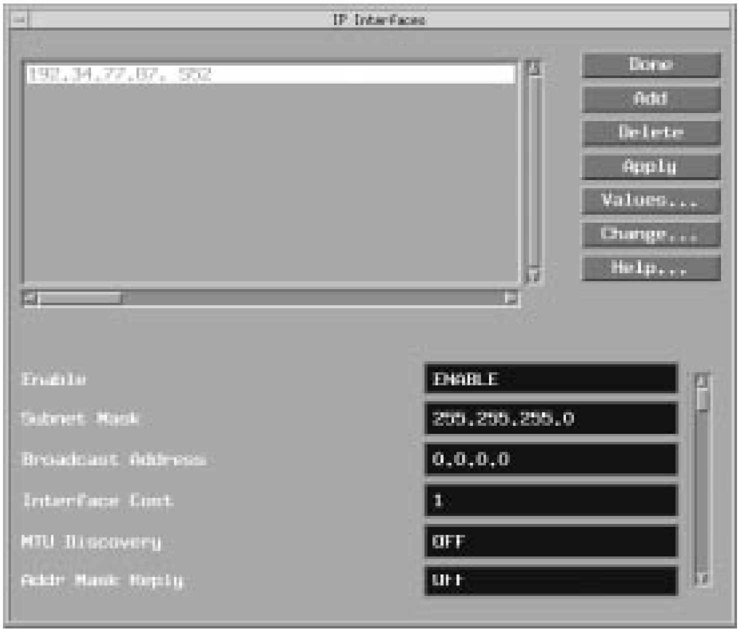
   The Circuit List window opens (refer to Figure 3-11).

2. **Select the circuit for multinet configuration, then click on Edit.**

The Circuit Definition window opens (refer to Figure 3-12).

3. **Choose Protocols** > **Edit IP** > **Interfaces.**

   The IP Interfaces window opens (Figure 3-13).



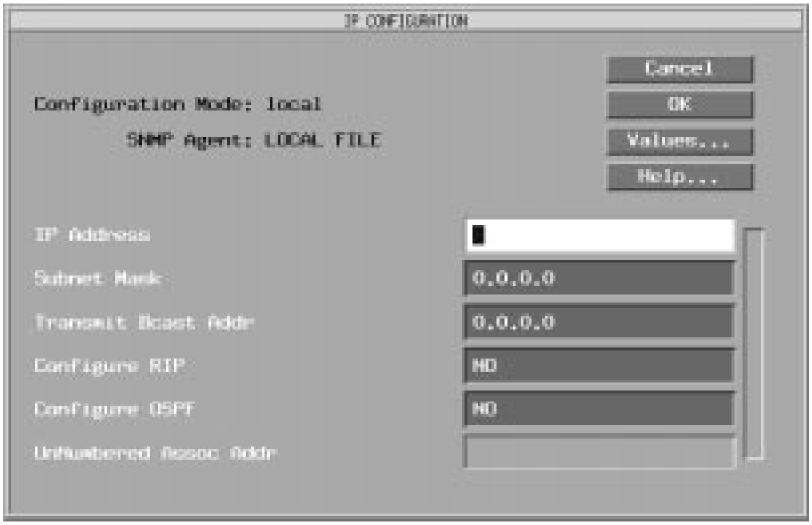
192.34.77.87, 552

Enable ENABLE
Subnet Mask 255.255.255.0
Broadcast Address 0.0.0.0
Interface Cost 1
MTU Discovery OFF
Addr Mask Reply OFF

Figure 3-13. IP Interfaces Window

4. **Click on Add.**

   The IP Configuration window opens (Figure 3-14).



Configuration Mode: local

SNMP Agent: LOCAL FILE

IP Address

Subnet Mask 0.0.0.0

Transmit Bcast Addr 0.0.0.0

Configure RIP NO

Configure OSPF NO

Unnumbered Assoc Addr

Figure 3-14. IP Configuration Window

5. **Specify an IP address for this circuit.**
6. **Click on OK.**

   You return to the IP Interfaces window (refer to Figure 3-13). The address you assigned to the circuit appears in the window’s list box.
7. **Repeat steps 1 through 6 for each IP address you want to add.**

Deleting Protocols from a Circuit

To delete protocols from a circuit:

1. **In the Configuration Manager window, choose Circuits > Edit Circuits.**

   The Circuit List window opens (refer to Figure 3-11).

2. **Select the circuit whose configuration you want to modify.**

3. **Click on Edit.**

   The Circuit Definition window opens (refer to Figure 3-12).

4. **Choose Protocols** > **Add/Delete.**

   The Select Protocols window opens (refer to Figure 3-9).

5. **Click on the box to the left of each protocol that you want to delete.**

6. **Click on OK.**

   You return to the Circuit Definition window (refer to Figure 3-12). The protocols you just deleted no longer appear in the Protocols list.

7. **Repeat steps 4 through 6 to delete other protocols.**

8. **Choose File > Exit.**

   You return to the Circuit List window.

9. **Click on Done.**

   You return to the Configuration Manager window.

Deleting a Circuit from the Router

When you delete a circuit from the router, you remove all line and protocol information from that circuit. If you want to redefine this circuit, you must repeat the procedure for adding network interfaces.

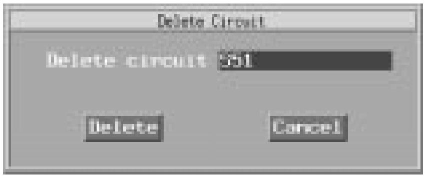
To delete a circuit from the router:

1. **In the Configuration Manager window, choose Circuits > Delete Circuit.**

   The Circuit List window opens (refer to Figure 3-11).

2. **Choose the circuit you want to delete.**
3. **Click on Delete.**

   The Delete Circuit window opens (Figure 3-15). The circuit you selected is displayed in the Delete circuit field.



Delete circuit S51

Figure 3-15. Delete Circuit Window

4. **Click on Delete again.**

   You return to the Circuit List window.

5. **Repeat steps 2 through 4 for each circuit that you want to delete.**
6. **Click on Done.**

   You return to the Configuration Manager window.

   The Configuration Manager deletes the circuit from the router. This circuit will no longer appear in the Circuit List window.

Modifying Configurations with New Link or Net Modules

When you replace a link module or net module with a module of a different type, you must edit the router's configuration file to reflect this change. When you change hardware in a slot containing configured circuits, the Configuration Manager automatically deletes the circuits.

Note: Only the ASN router uses net modules.

To replace a new link module or net module:

1. **Copy the router's configuration file.**

   Refer to "Making a Copy of the Existing Configuration File" on page 3-7.

2. **In the main Site Manager window, choose Tools > Configuration Manager > Local File/Remote File/Dynamic.**

   The Configuration Manager window opens (refer to Figure 3-7).

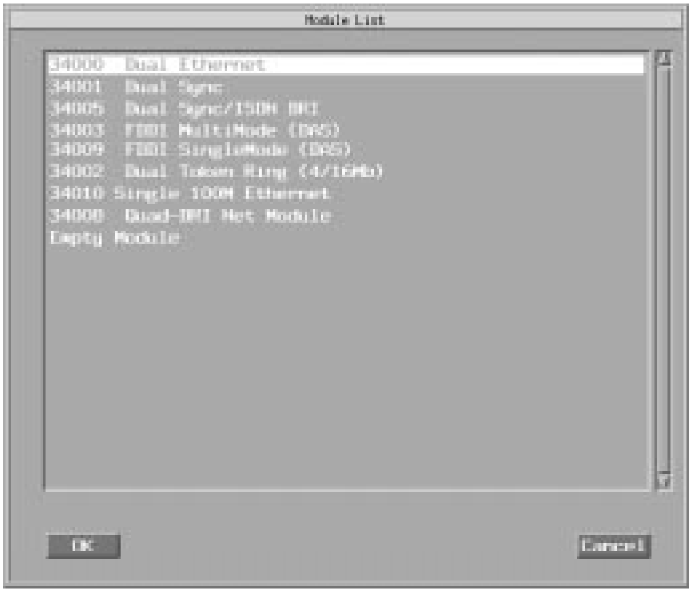
3. **Select the file and click on Open File.**

   The Configuration Manager displays the router's connectors.

4. **Specify the new module in the Configuration Manager window as follows:**

   a. **Click on the link or net module from which you deleted the circuits.**

      The Module List window opens. Figure 3-16 shows the Module List window for an ASN router.



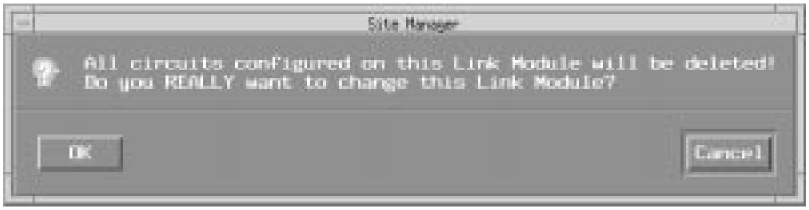
Module List

34000 Dual Ethernet
34001 Dual Sync
34005 Dual Sync/ISDN BRI
34003 FDDI MultiMode (DAS)
34009 FDDI SingleMode (DAS)
34002 Dual Token Ring (4/16Mb)
34010 Single 100M Ethernet
34008 Quad-BRI Net Module
Empty Module

Figure 3-16. Module List Window

b. **Select the new link module or net module you installed, then click on OK.**

   A confirmation window opens (Figure 3-17).



Site Manager

All circuits configured on this Link Module will be deleted!
Do you REALLY want to change this Link Module?

Figure 3-17. Confirming a Circuit Delete Request

c. **Click on OK.**

   You return to the Configuration Manager window (refer to Figure 3-7).

5. **Configure circuits on the new link or net module.**

   Refer to “Configuring a Circuit” on page 3-12.

6. **Choose File** > **Save to save your changes.**

   Refer to “Saving Configuration Files” on page 3-30 for instructions.

7. **Reboot the router with the edited configuration file.**

   Refer to Chapter 4 for instructions.

8. **Delete the old configuration file from the router.**

   Refer to Chapter 4 for instructions.

9. **Rename the edited configuration file to *config*.**

   Refer to Chapter 4 for instructions.

Saving Configuration Files

The Configuration Manager does not create a configuration file until you save the configuration information to a volume on the router's file system. A *volume* is the slot location of the router's flash memory card or the disk drive. Refer to one of the following sections for instructions on saving a configuration file. The instructions you choose should match the operating mode you selected when you started the Configuration Manager.

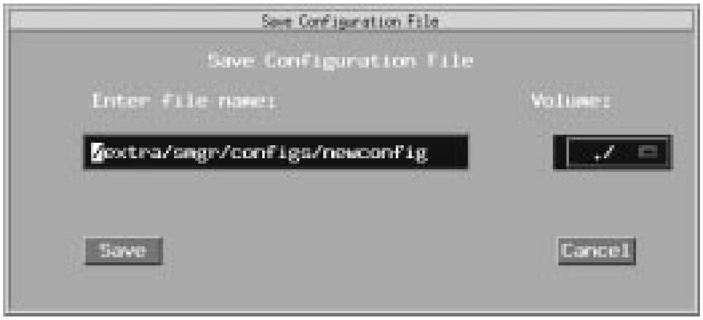
Caution: Before you save a new file, make sure that there is enough space in the router's memory. If you transfer a new file to the router, and the router cannot accommodate it, you will corrupt the new file. If the new file has the same name as the existing file, you will overwrite the existing file.

Saving a Configuration File in Local Mode

To save a configuration file created or modified in local mode:

1. **In the Configuration Manager window, choose File > Save As.**

   The Save Configuration File window opens (Figure 3-18).



Enter file name: /extra/smgr/configs/newconfig

Volume: ./

Figure 3-18. Save Configuration File Window

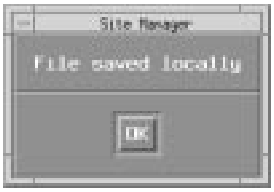
2. **Type a directory path, including the file name in the format *filename.cfg*, for example, *test.cfg*.**

   Save the file in a directory other than the one where Site Manager resides.

3. **Specify the appropriate directory by clicking on Volume and selecting a volume.**

4. **Click on Save.**

   The File Saved window opens (Figure 3-19).



File saved locally

Figure 3-19. File Saved Window

5. **Click on OK.**

   You return to the Configuration Manager window.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

7. **Go to the next section "Transferring a Local Mode Configuration File to the Router" to send the configuration file to the router.**

Transferring a Local Mode Configuration File to the Router

After you save a configuration file in local mode, you must transfer the file to the router before you can reboot the router with it. The Router Files Manager lets you transfer files between the Site Manager workstation and any Bay Networks router using the Trivial File Transfer Protocol (TFTP).

To transfer files from the Site Manager workstation to a router:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

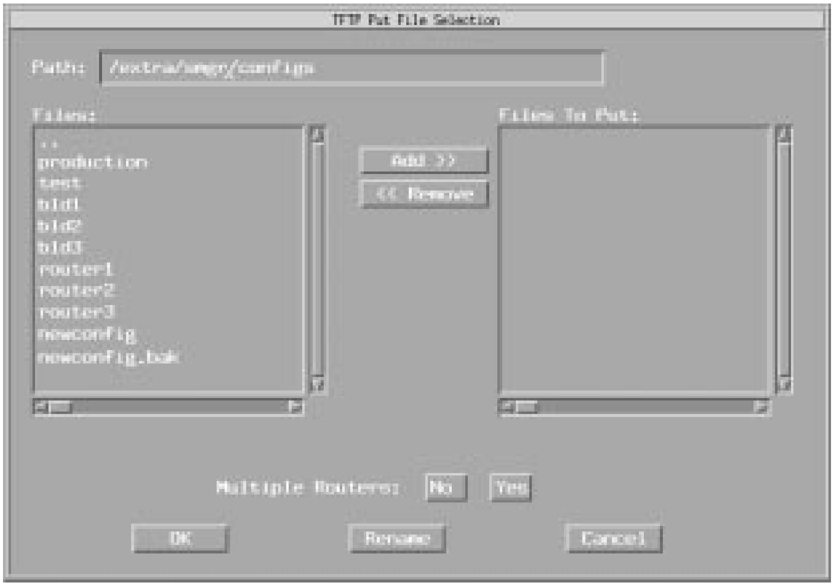
2. **Select a router volume.**

3. **Choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 3-1).

4. **Choose File > TFTP > Put File(s).**

   The TFTP Put File Selection window opens (Figure 3-20).



Path: /extra/smgr/configs

Figure 3-20. TFTP Put File Selection Window

5. **In the Path field, type the path to the directory that contains the file you want to transfer.**

   The files in that directory appear in the Files window. You may transfer one or more files at a time.

6. **In the Files list, click on the file that you want to transfer, then click on Add.**

   The selected file appears in the Files To Put list box.

   If you inadvertently add files that you do not want to transfer, select those files in the Files To Put list box and click on Remove.

7. **Repeat steps 5 and 6 to select files from other directories.**

8. **Click on No in the Multiple Routers field to send a file to only one router. Click on Yes to send it to multiple routers, provided you have set up the multiple routers option.**

   Refer to Chapter 5 for instructions on setting up multiple routers.

9. **Click on OK.**

The Router Files Manager transfers the selected file to the router.

During the file transfer operation, the Router Files Manager displays a message at the bottom of the window indicating which file is currently being transferred, and the address of the router that is receiving the file. When the transfer is complete, the TFTP Put File Selection window closes and you return to the Router Files Manager window.

10. **Go to Chapter 4 to boot the router with the new file.**

    You should test the configuration file to verify its integrity. After you are confident that you can use the new file, you can rename it *config*.

Saving a Configuration File in Remote Mode

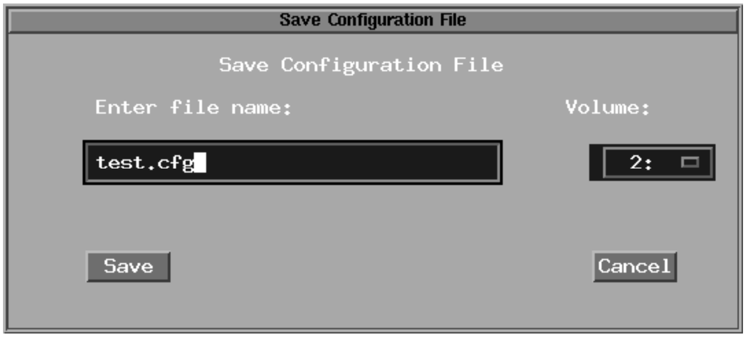
These instructions tell you how to save a configuration file in remote mode.

⛔ **Caution:** Do *not* use the file name *config* until you have tested the new configuration file.

To save a configuration file in remote mode:

1. **In the Configuration Manager window, choose File > Save As.**

   The Save Configuration File window opens (Figure 3-21).



Save Configuration File

Save Configuration File

Enter file name: test.cfg

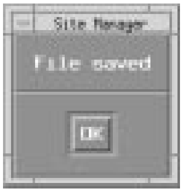
Volume: 2:

Figure 3-21. Save Configuration File Window

2. **Type a new file name using the format *filename.cfg*.**
3. **Select the destination volume for the file in the Volume field.**

4. **Click on Save.**

   The File Saved window opens (Figure 3-22).



File saved

Figure 3-22. File Saved Window

5. **Click on OK.**

   You return to the Configuration Manager window.

6. **Go to Chapter 4 to boot the router with the new file.**

   You should test the configuration file to verify its integrity. After you are confident that you can use the new file, you can rename it *config*.

Saving a Configuration File in Dynamic Mode

If you make configuration changes in dynamic mode, you are changing the active configuration file on the router. You are implementing changes in memory, but not overwriting the *config* file until you save the modified file. When you save your changes, the file is saved directly to the router. Save dynamically made changes to the *config* file only when you want to maintain a permanent record of the changes.

To save your changes:

1. **In the Configuration Manager window, choose File > Save As.**

   The Save Configuration File window opens (refer to Figure 3-21).

2. **Enter a new file name, using the format *filename.cfg*.**

   If you use a unique file name, you will not overwrite the existing *config* file.

3. **Select the correct volume by clicking in the Volume field.**

4. **Click on Save.**

   The File Saved window opens, asking you to confirm your decision to save the file (refer to Figure 3-22).

5. **Click on OK.**

Chapter 4
Booting the Router

To restart the router with a modified configuration file or router image file, or to recover if the router experiences a problem, you need to boot the router. In this book, the term *boot* refers to a warm-start of the router. When you warm-start a router, the power remains on while the router resets; you do not use the power switch to turn the router off and then on.

This chapter contains the following information:

Booting Methods

You can boot the router in one of three ways:

- Regular boot (also referred to as a default boot)

  The router boots with the default *config* and image files when you press the Reset button on the router.

- Named boot

  The router boots with configuration and image files that you name.

- Scheduled boot

  The router boots with configuration and image files that you name at a time of day that you specify.

In addition to booting the router as a whole, you can boot an individual hardware module by resetting the module.

➡ **Note:** For the AN, ANH, ASN and ARN routers, you can also use EZ-Install, Netboot, or Directed Netboot to boot the router. For information about these boot procedures, refer to the appropriate router documentation.

Preparing to Boot a Router

You access the boot function in the main Site Manager window by choosing Administration from the main menu bar.

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 turn off and then turn on the router, or use the Technician Interface **diags** command. Refer to *Using Technician Interface Software* for information about the **diags** command.

Booting interrupts router operation, so plan your boot carefully. Before you boot the router, decide the following:

- Which router you are booting
- Whether to use the default configuration and image files, or files you specify
- Whether to use a scheduled boot

FN/LN/CN Router Boot Prerequisite

The PCMCIA/Floppy switch on the Flash System Controller board of an FN®, LN®, or CN® router determines where the router looks for the image (*ace.out*) and configuration file when it is booting. The PCMCIA 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 to the PCMCIA position.

When you use Site Manager to boot the router, or when you specify an image and configuration file in a Technician Interface **boot** command, the software verifies the files' 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:

- The router boots using *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.
- The router boots using *1:config* if it is available. If not, it boots from *2:config* if it is available. If both are unavailable, a configuration error occurs.

Booting with the Default Configuration and Image Files

To boot the router using the default configuration file (*config*) and image file, press the Reset button on the router's front panel.

You typically perform this type of boot when testing a new configuration file. If the router does not boot properly, you can press the Reset button to boot the router using the default *config* file.

Booting with a Named Boot

You typically perform a named boot to use a new or modified configuration or image file. This type of boot lets you specify the files that the router uses to boot and to operate.

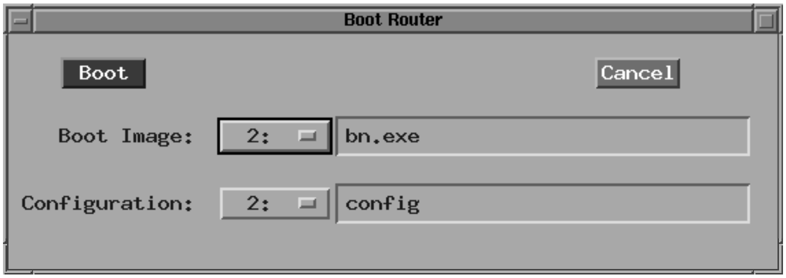
If you are booting with a new or modified configuration file, you should have saved this file under a unique name. (Refer to Chapter 3 for instructions on how to save a configuration file.) After you boot the router with the new file and are confident that it is stable, you can then rename the file *config,* the default configuration file.

To perform a named boot:

1. **In the main Site Manager window, choose Administration > Boot Router.**

   The Boot Router window opens listing the default volumes and file names for the router boot image and the configuration file (Figure 4-1). The file names and volumes vary depending on the router.

   For routers that use flash memory cards or single inline memory modules (SIMMs), the default volume is the first available card or module, which is designated by its slot number. For routers that use diskettes, the volume is the letter A.



Boot Image: 2: bn.exe

Configuration: 2: config

Figure 4-1. Boot Router Window

2. **To use a boot image and configuration file other than the ones displayed, go to step 3. To accept the files listed, go to step 4.**

3. **For a router with multiple volumes, specify the volume for the boot image and the volume for the configuration file.**

   a. **Click in the volume box for the boot image (not the box that displays the name of the boot image file, for example, *bn.exe*).**

      A menu lists all available volumes.

   b. **Choose the volume with the boot image that you want to use.**

   c. **To boot with a different image file, type the file name in the field next to the volume box.**

   d. **Repeat steps a through c for the configuration file volume and name.**

4. **Click on Boot.**

   A confirmation window appears.

5. **Click on OK.**

   The router boots using the router software image and the configuration file you specified.Wait a few minutes for the router to boot.

6. **In the main Site Manager window, choose View** > **Refresh Display to verify that the router booted correctly.**

   If the router booted correctly, the new system information appears in the main Site Manager window.

   If Site Manager does not display system information, the router did not boot successfully. Contact your local Bay Networks Technical Solutions Center for assistance.

   If you can no longer access the router with Site Manager, refer to *Using Technician Interface Software* for instructions on using the Technician Interface to access the router. Contact your local Bay Networks Technical Solutions Center for assistance.

7. **If you are confident the configuration file is stable, go to the next section, "Copying and Renaming the Configuration File."**

Copying and Renaming the Configuration File

By default, the file named *config* is the configuration file used to boot the router. After you test a modified configuration file, you can use the Router Files Manager to copy the file under the default file name, *config*, and delete the old file.

Before you copy your configuration file, make sure that there is enough space on the router for all the files. Refer to Chapter 5 for information.

To copy and rename a modified configuration file:

1. **In the main Site Manager window, choose Tools** > **Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 3-1).

2. **Choose the router volume where the configuration file resides.**
3. **Choose the modified configuration file from the list of files.**
4. **Choose Commands** > **Copy.**

   The Copy window opens (refer to Figure 3-3).

5. **Click on OK.**

   A second Copy window prompts you for the destination file name (refer to Figure 3-4).

6. **Enter *config* in the window, then click on OK.**

   A confirmation window opens.

7. **Click on OK.**

   You return to the Router Files Manager window.

   The modified configuration file has been copied and renamed *config*, overwriting the existing *config* file.

8. **Go to the next section, "Deleting a Configuration File," to delete the test configuration file.**

Deleting a Configuration File

Use the Router Files Manager to delete a configuration file from the router, that is, the test configuration file, not the *config* file.

To delete a file:

1. **In the Site Manager window, choose Tools** > **Router Files Manager.**

   The Router Files Manager window opens.

2. **Select the test configuration file from the list.**

3. **Choose Commands** > **Delete.**

   A confirmation window appears.

4. **Click on OK.**

   The Router Files Manager deletes the file.

5. **If the router uses flash memory, choose Commands** > **Compact to compact memory.**

Booting with a Scheduled Boot

A scheduled boot, or Remote User Interface (RUI) boot, lets you specify the exact date and time a boot takes place. It functions in all other aspects as a named boot (refer to “Booting with a Named Boot”).

This section describes how to:

- Enable and disable a scheduled boot.
- Schedule multiple boot times.
- Modify a scheduled boot.
- Delete a scheduled boot.

Enabling and Disabling a Scheduled Boot

Setting up a scheduled boot involves:

- Enabling the boot
- Configuring the boot schedule

You can globally enable and disable a scheduled boot. A scheduled boot will not take place until you enable it; however, you can configure the boot schedule even if the boot is disabled. Disabling a boot does not alter the boot schedule; the boot will occur after you reenable it. If the scheduled boot is enabled later, any routers whose boot time has not expired will boot as scheduled.

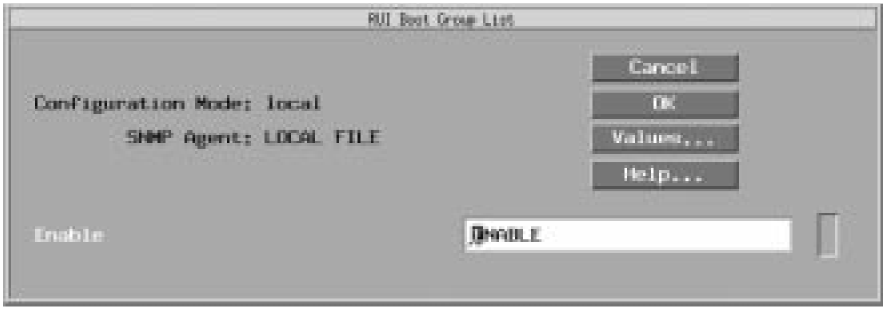
To enable and disable a scheduled boot:

1. **In the Site Manager window, choose Tools > Configuration Manager.**

   The Configuration Manager window opens.

2. **In the Configuration Manager window, choose Platform > Scheduled Boot > Create Boot Param.**

   The RUI Boot Group List window opens (Figure 4-2).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Enable ENABLE

Figure 4-2. RUI Boot Group List Window

3. **Edit the parameter.**

   -- Enter Enable to globally enable booting.

   -- Enter Disable to globally disable booting.

   After you enable the boot parameter, you choose Platform > Scheduled Boot > Global to enable or disable subsequent scheduled boots.

4. **Click on OK.**

   You return to the Configuration Manager window.

Configuring the Boot Schedule

To specify the date and time for a router boot, as well as the image and configuration files the router uses:

1. **In the Configuration Manager window, choose Platform > Scheduled Boot > Boot Parameters.**

   The RUI Boot Interface Parameters window opens (Figure 4-3).

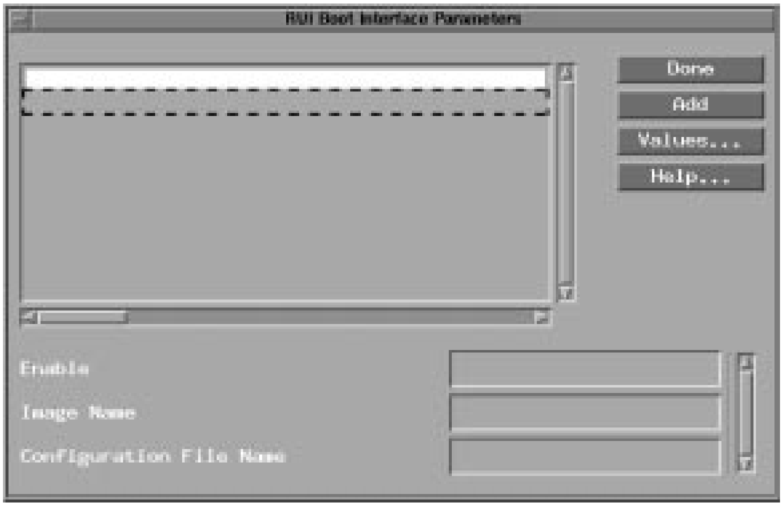
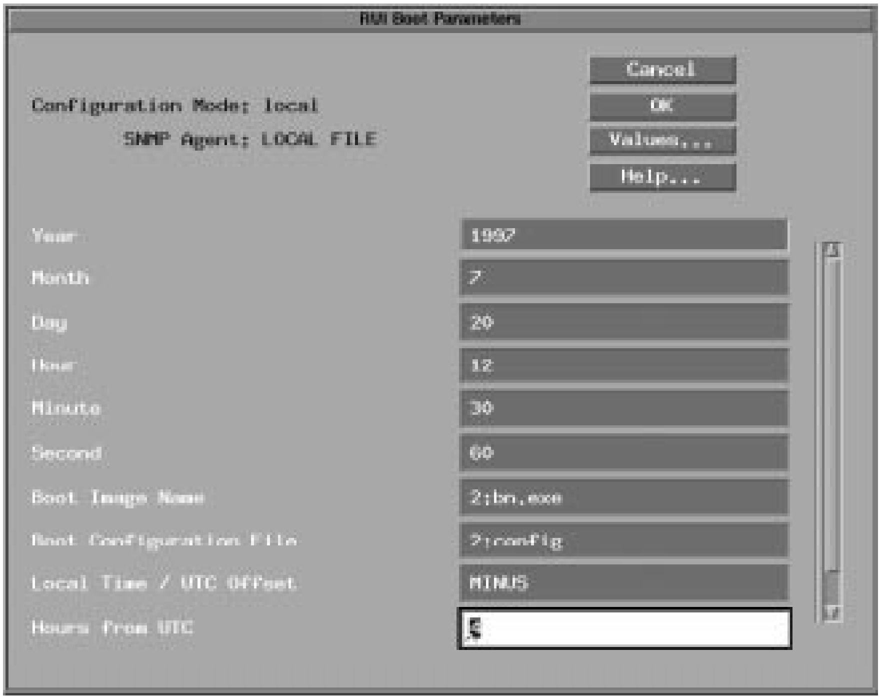


Figure 4-3. RUI Boot Interface Parameters Window

2. **Click on Add.**

   The RUI Boot Parameters window opens (Figure 4-4).



RUI Boot Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

Year	1997
Month	7
Day	20
Hour	12
Minute	30
Second	60
Boot Image Name	2:bn.exe
Boot Configuration File	2:config
Local Time / UTC Offset	MINUS
Hours From UTC	5

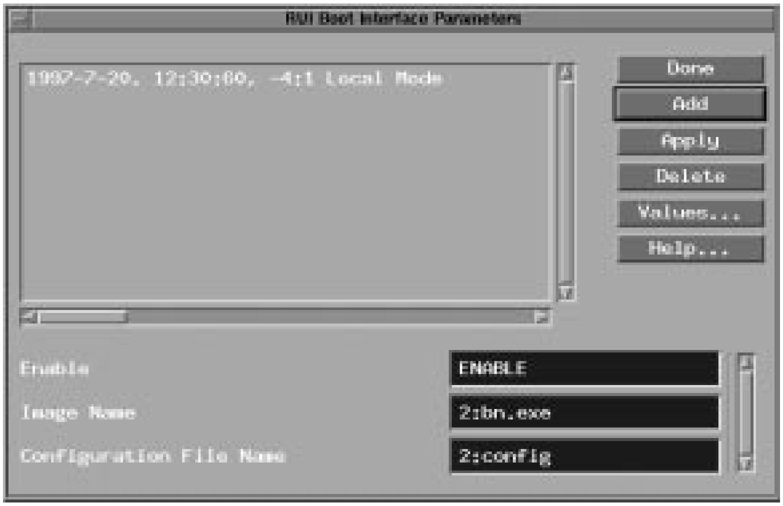
Figure 4-4. RUI Boot Parameters Window

3. **Enter the appropriate information for each of the parameters.**

   You must configure all the parameters to schedule a boot. Refer to the parameter descriptions beginning on page B-12 or click on Help.

4. **Click on OK.**

   You return to the RUI Boot Interface Parameters window, which lists the image name and configuration file of the appropriate router (Figure 4-5). The date and time of the boot appear in the list box.



1997-7-20, 12:30:60, -4:1 Local Mode

Enable ENABLE

Image Name 2:bn.exe

Configuration File Name 2:config

Figure 4-5. RUI Boot Interface Parameters Window

5. **Click on Done.**

   You return to the Configuration Manager window.

   A scheduled boot is now configured for the specified date and time, using the boot image and configuration file you specified.

How the Router's Date and Time Affect a Scheduled Boot

If you change the router's date and time after you configure a scheduled boot, the router does not adjust the boot schedule accordingly. The router boots based on the previous date and time.

For the router to boot as scheduled, you must delete the original boot schedule and create a new one that works with the router's new date and time.

Modifying the Parameters for a Scheduled Boot

You can modify the Enable, Image Name, and Configuration File Name parameters for a scheduled boot. To modify the date and time of a scheduled boot, you must delete that boot and reschedule another boot. Refer to“Deleting a Scheduled Boot,” next in this chapter, for instructions.

To edit parameters for a scheduled boot:

1. **In the Configuration Manager window, choose Platform > Scheduled Boot > Boot Parameters.**

   The RUI Boot Interface Parameters window opens (refer to Figure 4-5).

2. **Select the entry you want to modify from the list.**
3. **Edit the Enable, Image Name, or Configuration File Name field.**

   Refer to the parameter descriptions on page B-12 or click on Help.

4. **Click on Apply.**
5. **Click on Done.**

   You return to the Configuration Manager window.

Deleting a Scheduled Boot

To modify the date and time of a scheduled boot, you must delete the original boot schedule and create a new one. You can delete individual boot entries or all of them. The sections that follow describe each method.

Deleting Individual Scheduled Boots

To delete an individual boot entry:

1. **In the Configuration Manager window, choose Platform > Scheduled Boot > Boot Parameters.**

   The RUI Boot Interface Parameters window appears (refer to Figure 4-5).

2. **Choose the scheduled entry you want to delete.**
3. **Click on Delete.**

   The boot entry is deleted.

4. **Click on Done.**

   You return to the Configuration Manager window.

5. **To create a new scheduled boot entry, refer to “Booting with a Scheduled Boot” on page 4-9.**

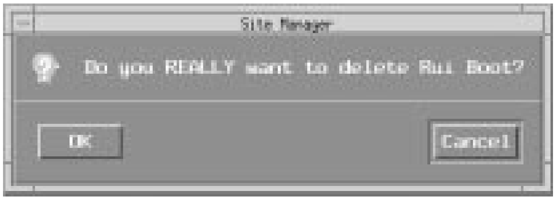
Deleting All Scheduled Boots

You can delete all scheduled boots from the current version of Site Manager. After you delete all entries, you cannot recover them. To disable all scheduled boots without deleting them, refer to “Enabling and Disabling a Scheduled Boot” on page 4-9.

To delete all scheduled boots:

1. **In the Configuration Manager window, choose Platform > Scheduled Boot > Delete.**

   The Delete RUI Boot message window opens (Figure 4-6).



Do you REALLY want to delete Rui Boot?

Figure 4-6. Delete RUI Boot Message Window

2. **Click on OK.**

   The Configuration Manager deletes all scheduled boot entries.

   You return to the Configuration Manager window.

Booting a Processor Module

To troubleshoot a router problem, you can boot a processor module to determine whether the module is the problem. To boot an individual processor module, you use the Reset Slot option in the Administration menu in the Site Manager menu bar. The Reset Slot option warm-starts a single processor module in the router with the boot image and configuration file that the router is currently using.

The following steps explain what happens when you boot a processor module:

1. The router software that is operating on the processor module forwards a boot request to the other processor modules.
2. The first processor module that responds to the boot request sends back the boot image resident in its memory to the requesting module.
3. The processor module that you are booting receives and executes the boot image. The router disrupts connectivity to the associated slot and to the services provided by that slot. The other processor modules resynchronize their routing tables after the slot fails to receive packets.
4. The processor module that you are booting completes the boot process and requests a configuration. The first available processor module sends the configuration resident in its memory.
5. The resetting processor module loads the configuration image and initiates the services provided by the slot, thus reestablishing connectivity. It then alerts the other processor modules that it can receive packets.
6. The other processor modules resynchronize their routing tables accordingly.

To boot a processor module:

1. **In the main Site Manager window, choose Administration > Reset Slot.**

   The Reset Slot window opens, showing the router's default slot (Figure 4-7).

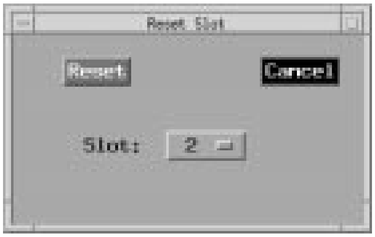


Figure 4-7. Reset Slot Window

2. **Click on the box displaying the slot number.**

   A menu opens listing all available slots (Figure 4-8).

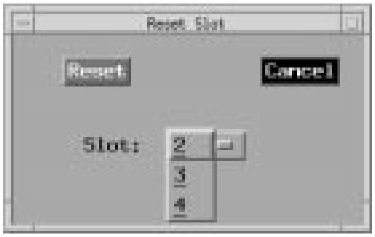


Figure 4-8. Selecting a Slot

3. **Choose the slot that holds the processor module that you want to boot.**
4. **Click on Reset.**

   A confirmation window opens.
5. **Click on OK.**

   You return to the main Site Manager window.

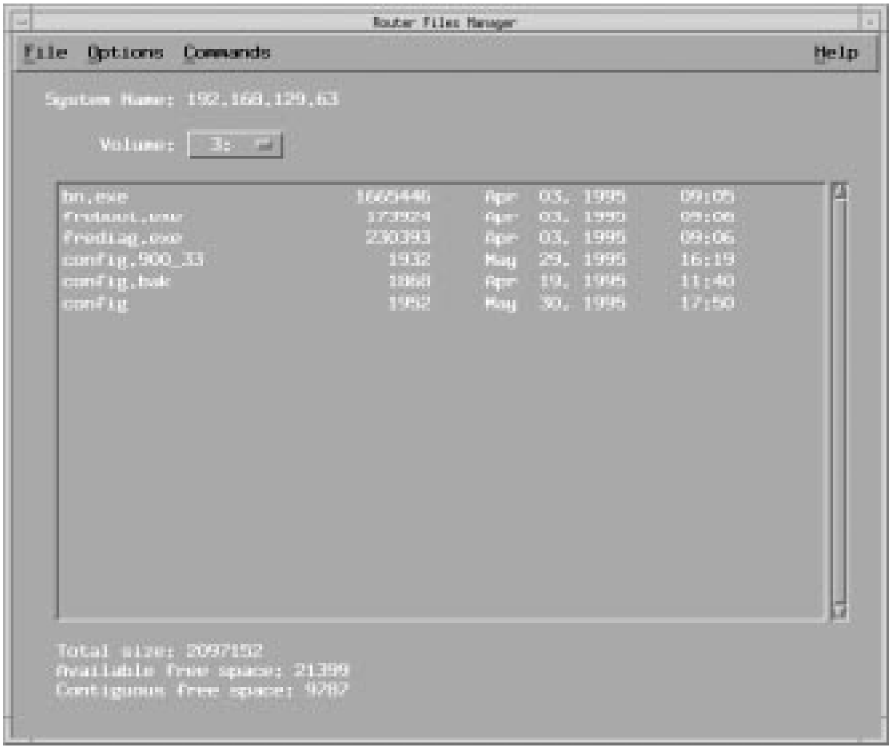
Chapter 5
Managing Router Files

To manage router files, you use the Router Files Manager. To access the Router Files Manager, choose Tools > Router Files Manager from the main Site Manager window.

This chapter contains the following information:

Displaying a List of Router Files

To display the files on the router, begin at the main Site Manager window and choose select Tools > Router Files Manager. The Router Files Manager window opens, showing the files in the active volume (Figure 5-1).



System Name: 192.168.129.63

Volume: 3:

```
bn.exe              1665446    Apr  03, 1995    09:05
freboot.exe          173924    Apr  03, 1995    09:06
frediag.exe          230393    Apr  03, 1995    09:06
config.900_33          1932    May  29, 1995    16:19
config.bak             1868    Apr  19, 1995    11:40
config                 1952    May  30, 1995    17:50
```

```
Total size: 2097152
Available free space: 21399
Contiguous free space: 9787
```

Figure 5-1. Router Files Manager Window

Note: You can access the same window from the main Site Manager window by clicking on the Files button.

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 (Table 5-1).

Table 5-1. Active Volume Representations

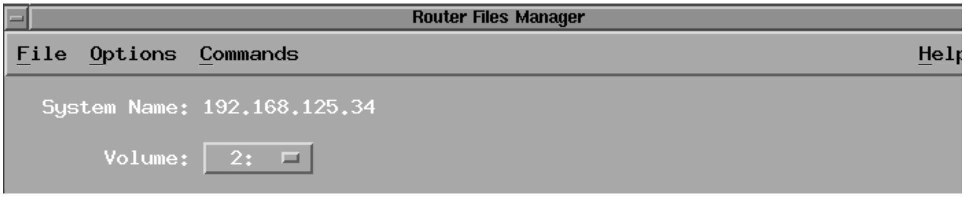
Media	Active Volume	Description
Flash memory card or SIMM	1 through 14[a]	If the router uses a memory card or a SIMM, the active volume can be from 1 through 14, depending on the router platform.
Diskette	A	If the router uses a diskette, the active volume shown is A.

[a] This number is the number of the slot where the first available memory card resides. Additional memory cards in the router are optional; they provide redundancy and additional storage.

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 AN, ANH, and ASN Routers" on page 5-25.

To change the volume displayed, click in the Volume box just above the list of files in the Router Files Manager window (Figure 5-2). The Volume box lists all available volumes on the router. Choose the volume you want.

For PC users, not all the volumes will be visible when you click in the Volume box. Use the arrows to the right of the volume number to scroll through the list of available volumes.



System Name: 192.168.125.34

Volume: 2:

Figure 5-2. Volume Box in Router Files Manager Window

Default Router File Names

Table 5-2 lists the default file names in the Router Files Manager window.

Table 5-2. Default Router File Names

File Name	Description	Notes
ace.out	Bootable image for the FN, LN, ALN, AFN with diskette, and CN	The router 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 file name for the router to boot successfully after a cold-start. Using the Administration > Boot Router option, you can specify another software image. You can rename the bootable image file, but you must use the new name when you boot the router. See Chapter 4 for information about booting routers.
afn.exe	Bootable image for the AFN with nonvolatile (flash) file system	
an.exe	Bootable image for the AN and ANH	
arn.exe	Bootable image for the ARN	
asn.exe	Bootable image for the ASN	
bn.exe	Bootable image for the BLN and BCN	
s5000.exe	Bootable image for the System 5000	
asndiag.exe	Copy of the diagnostics image for the ASN	You cannot read or change this file.
bcc.help	Help file for the Bay Command Console (BCC™)	You cannot change this file.
config	Default configuration file	The router references this binary file for configuration data when booting. You can use another configuration file using the Boot Router option. You can change the default *config* file by renaming a new, tested configuration file to *config*. The file must be named *config* for the router to boot with it automatically. We recommend that you back up the *config* file under a unique name before overwriting it.
debug.al	ASCII file containing aliases	Aliases are commands that abbreviate long or multiple commands. They are used to debug common network problems.
frediag.exe	Copy of the diagnostics image resident on the diagnostics PROM for the BCN and BLN	You cannot read or change this file.

(continued)

Table 5-2. Default Router File Names *(continued)*

File Name	Description	Notes
freboot.exe	Copy of the bootstrap image resident on the bootstrap PROM for the BCN and BLN	You cannot read or change this file.
install.bat	Script containing Technician Interface commands	You use Bay Networks Technician Interface commands during the initial startup. Refer to *Quick-Starting Routers*.
ti.cfg	Configuration file containing the MIB variables associated with the default Technician Interface 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.

File-Naming Conventions

Table 5-2 lists the default file names for the router software. You can change file names or make copies of a file and give the copy a unique name. For example, if you modify a configuration file, you may want to test it under a unique name before you rename it *config* and overwrite the original configuration file.

The guidelines for naming files are:

- File names must start with an alphabetical character. The remaining characters must be alphanumeric and may also include the underscore (_) character.
- Image file names can consist of 1 to 8 characters, while configuration file names can consist of 1 to 15 characters (including a period). Bay Networks recommends that you limit file names to 8 characters to ensure that all supported operating systems can recognize the names.
- File name extensions are optional and must be preceded by a file name and a period. They can be from 1 to 3 characters.

In addition to the previous guidelines, Bay Networks recommends that you use the following conventions when you name files so that you can distinguish files by type:

- Use the *.exe* extension for software images for FRE processor modules and *.out* for ACE processor modules (refer to Table 5-2).
- Use the *.cfg* extension for alternate configuration files. The default configuration file is *config*.
- Use the *.al* extension for alias files.
- Use the *.log* extension for log files.

Checking Available and Contiguous Free Space on a Volume

At the bottom of the Router Files Manager window (refer to Figure 5-1), the amount of free space in a selected volume is displayed (Table 5-3).

Table 5-3. Free Space Information

Field	Description
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

The router volume must have enough space available for a copied or transferred file. Depending on the router software version you are using, your software may automatically check the available space for you. To display your router software version, choose Help > Site Manager Version in the Router Files Manager window.

Routers that use Version 7.80 software (or later) automatically check to ensure that there is adequate free space on the destination volume.

For routers that use software earlier than Version 7.80, do the following:

- Determine the size of the file you want to copy.
- Check the amount of free space available on the destination volume; free space is displayed at the bottom of the Router Files Manager window.

  For a router diskette destination volume, use the number of bytes displayed for the `Available free space`. For a flash memory destination volume, use the number of bytes displayed for `Contiguous free space`.

Caution: Copying a file to flash memory that has an insufficient amount of contiguous free space can corrupt the copied file. Before you copy a file, compact memory. Refer to “Compacting Flash Memory ” on page 5-22.

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. You may want to copy a file and modify it to protect the original.

Before you copy a file, do the following:

- Use a unique file name for the copy.

  The router automatically overwrites any existing file with a file of the same name. To avoid overwriting an existing file, display a list of the volume's contents and check the file names that are already in use. Refer to "Displaying a List of Router Files" on page 5-2 for instructions.

  If you are unfamiliar with the file-naming conventions, refer to "File-Naming Conventions" on page 5-6 before you proceed.

- Verify that you have adequate space on the destination volume.

  Refer to "Checking Available and Contiguous Free Space on a Volume" on page 5-7.

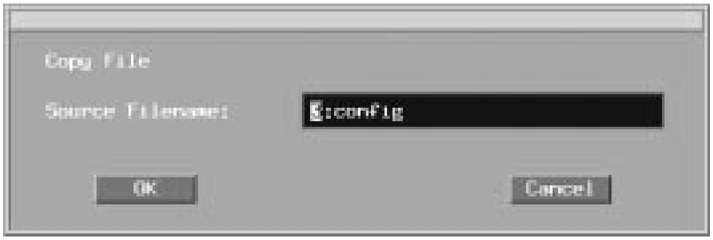
To copy a file on the router:

1. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

2. **Choose the volume where the source file resides.**
3. **Choose the file you want to copy.**
4. **Choose Commands > Copy.**

   The Copy window opens displaying the source file name (Figure 5-3).



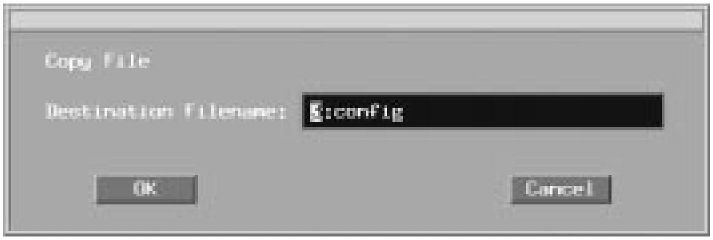
Copy File

Source Filename: 5:config

Figure 5-3. Copy Window (Source File Name)

5. **Click on OK.**

   A second Copy window prompts you for the destination file name (Figure 5-4).



Copy File

Destination Filename: B:config

Figure 5-4. Copy Window (Destination File Name)

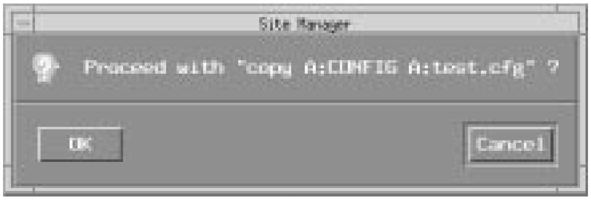
6. **Enter the destination file name in the following format:**

   <volume>:<file_name>

   If you are copying a file from a diskette to flash memory, enter the destination file name in lowercase letters only.

7. **Click on OK.**

   A confirmation window opens (Figure 5-5).



Site Manager

Proceed with "copy A:CONFIG A:test.cfg" ?

Figure 5-5. Copy Confirmation Window

8. **Click on OK.**

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

   You return to the Router Files Manager window.

Deleting a File

Using the Router Files Manager, you can delete one or more files at a time from a volume.

Caution: You cannot recover a file after you delete it. Be sure to back up critical files.

To delete files from a router:

1. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

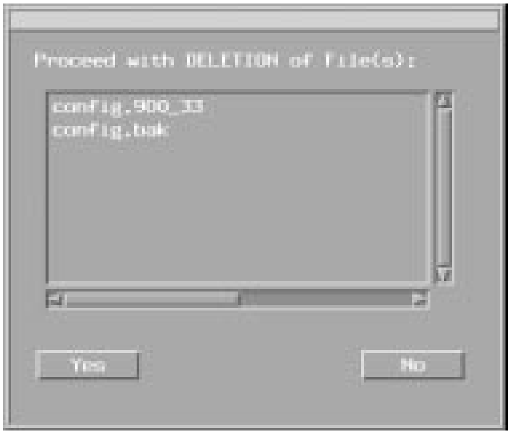
2. **Select the file that you want to delete.**

   To select multiple files, click on each file.

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

3. **Choose Commands > Delete.**

   A window prompts you to confirm your delete request (Figure 5-6).



Proceed with DELETION of File(s):

config.900_33
config.bak

Figure 5-6. Deleting Router Files

4. **Click on Yes.**

   The router deletes the files you specified from the volume.

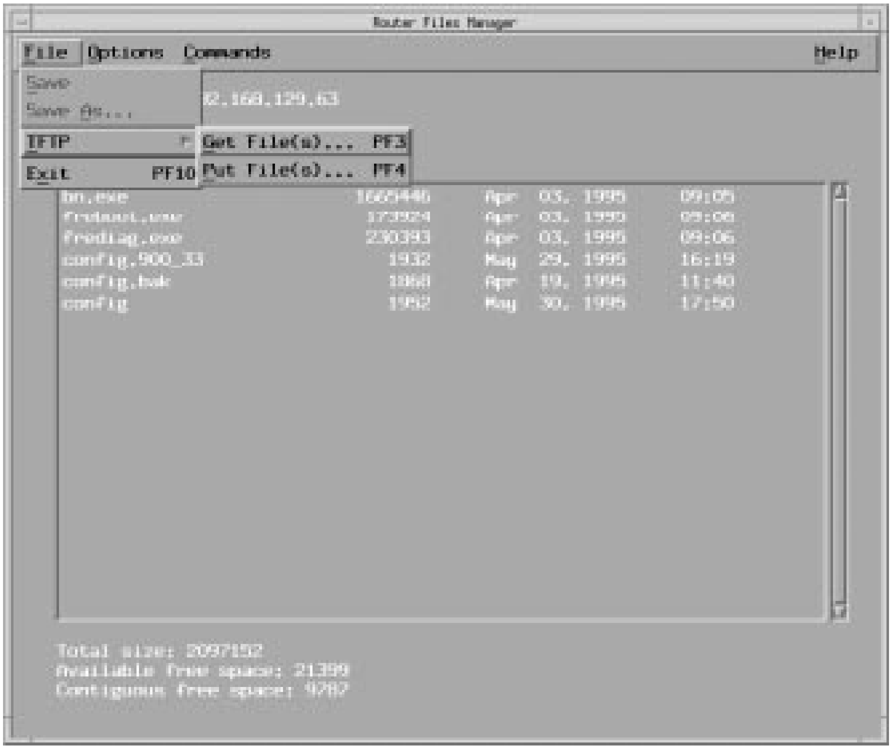
   You return to the Router Files Manager window.

5. **If the router uses flash memory, choose Commands** > **Compact to compact memory.**

   Compacting memory provides more file space and ensures that the available free space is contiguous.

Transferring Files

The Router Files Manager allows you to transfer files between any router and Site Manager workstation by using the Trivial File Transfer Protocol (TFTP) (Figure 5-7).



```
2.168.129.63

bn.exe                 1665446    Apr  03, 1995    09:05
frdaust.exe             173924    Apr  03, 1995    09:06
frediag.exe             230393    Apr  03, 1995    09:06
config.900_33             1932    May  29, 1995    16:19
config.bak                1868    Apr  19, 1995    11:40
config                    1952    May  30, 1995    17:50

Total size: 2097152
Available free space: 21399
Contiguous free space: 9787
```

Figure 5-7. Choosing the TFTP Option

Using TFTP, you can perform the following tasks:

- Transfer a file from the router to the Site Manager workstation (refer to “Transferring a File from the Router” on page 5-13).
- Transfer a file from the Site Manager workstation to the router (refer to “Transferring Files to the Router” on page 5-16).

.

➡ **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 adjust this parameter, duplicate transfer sessions may occur. This, in turn, may result in zero-length or locked files on the diskette. (For more information about how to set the TFTP Retry Time Out parameter, refer to *Configuring IP Utilities*.)

Transferring a File from the Router

The Get File(s) option from the TFTP menu allows you to transfer one or more files from the router to the Site Manager workstation. You can retrieve files from only one router at a time.

To transfer files from the router to the Site Manager workstation:

1. **In the Router Files Manager window, connect to the router.**

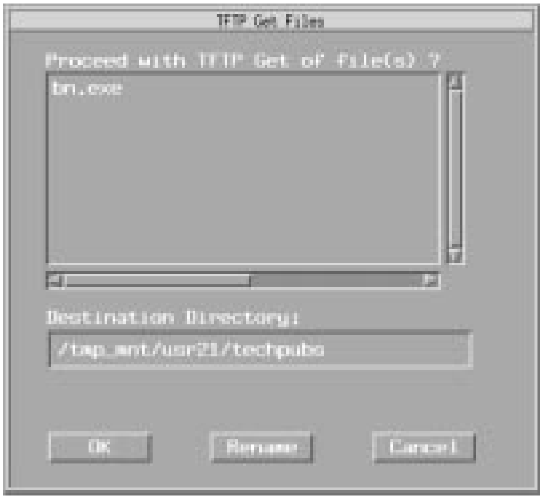
   Refer to Chapter 1 for instructions.

2. **Choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

3. **Select the router volume from which you need to transfer a file.**
4. **Select the files you want to transfer from the router.**
5. **Choose File > TFTP > Get File(s).**

   The TFTP Get Files window opens (Figure 5-8).



TFTP Get Files

Proceed with TFTP Get of file(s) ?

bn.exe

Destination Directory:

/tmp_mnt/usr21/techpubs

Figure 5-8. TFTP Get Files Window

6. **Transfer the files using one of the following methods:**

   - To transfer a file without changing the file name, specify the destination directory on the Site Manager workstation and click on OK.
   - The Router Files Manager transfers the file to the Site Manager workstation. If a file with the same name already exists in that directory, the transferred file overwrites it.
   - To transfer a file under a new name, click on Rename (Figure 5-8).

   The TFTP Rename Files window opens (Figure 5-9).

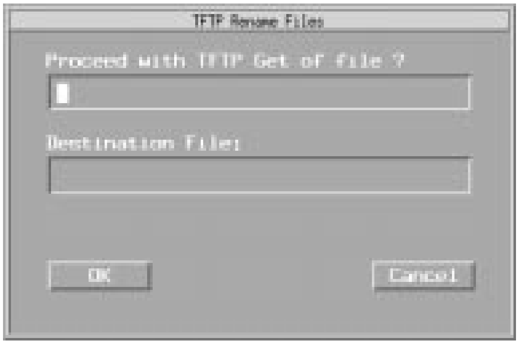


Figure 5-9. TFTP Rename Files Window

a. **Enter the name of the file you want to retrieve from the router in the Proceed with TFTP Get of file field.**

b. **Enter the path and file name of the destination directory on your Site Manager workstation in the Destination File field.**

c. **Click on OK.**

The Router Files Manager transfers the files to the Site Manager workstation using the new name. If a file with the same name already exists in that directory, the transferred file overwrites it.

Transferring Files to the Router

The Put File(s) option from the TFTP menu allows you to transfer files from the Site Manager workstation to one or more routers. Note the following guidelines:

- If the destination router is running IP in host-only mode, and you have configured the destination router with the same IP address on multiple physical interfaces, test the connection to the router using the ping command. After the connection is active you can transfer the file.
- Use a unique file name for the transferred file.

  The router automatically overwrites any existing file with a file of the same name. To avoid overwriting an existing file, display a list of the volume’s contents to check the file names that are already in use. Refer to “Displaying a List of Router Files” on page 5-2 for instructions.

  If you are unfamiliar with the file-naming conventions, refer to “File-Naming Conventions” on page 5-6 before you proceed.
- Verify that you have adequate space on the destination volume.

  If you transfer a new file that the router cannot accommodate, you will corrupt the new file. Refer to “Checking Available and Contiguous Free Space on a Volume” on page 5-7.

If you are transferring files to one router only, go to “Using the Put Files Option to Transfer Files” on page 5-19.

Setting Up File Transfers to Multiple Routers

You can transfer one or more files from the Site Manager workstation to several routers simultaneously. For example, you might want to send a new boot image to three different routers at the same time.

Before you can use the Put File(s) option to transfer files to multiple routers, you need to set up the destination routers.

To set up multiple routers to receive file transfers:

1. **In the Router Files Manager window, choose Options > Router Connection.**

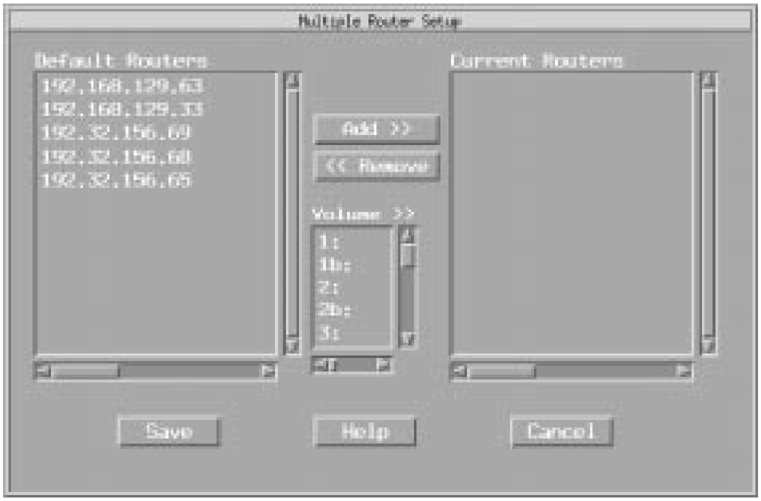
   The Router Connection Options window opens.

2. **Complete the Router Connection Options window for each router to which you want to transfer the files, then click on OK.**

   Refer to Chapter 1 for instructions on completing this window.

3. **Choose Options > Multiple Router Setup.**

   The Multiple Router Setup window opens (Figure 5-10).



Default Routers
192.168.129.63
192.168.129.33
192.32.156.69
192.32.156.68
192.32.156.65

Volume >>
1:
1b:
2:
2b:
3:

Figure 5-10. Multiple Router Setup Window

The Default Routers list displays the routers to which you are currently connected. The Current Routers list displays the routers whose files you want to manage simultaneously. The Volume list displays all the volume identifiers for Bay Networks routers.

4. **Select the destination volumes and routers for the files being transferred as follows:**

   a. **Select one or more routers from the Default Routers list.**

   b. **Select one or more volumes from the Volume list.**

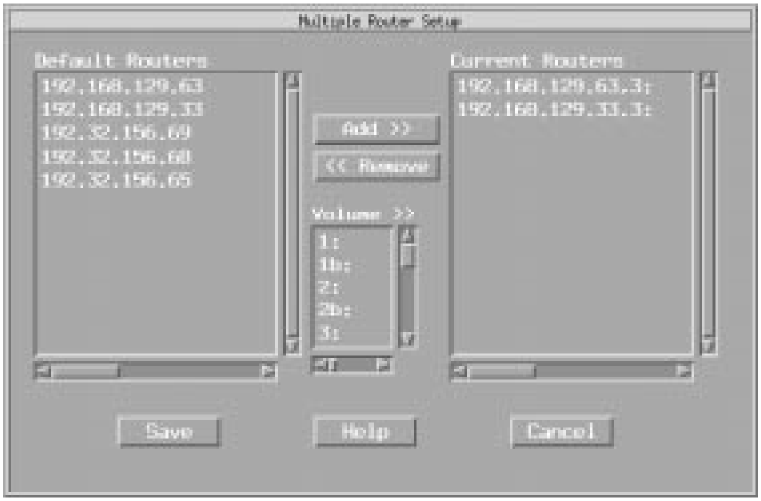
   -- Select only one volume to transfer files to the same volume on all the routers you selected.

   -- Select one or more volumes to transfer files to different volumes on multiple routers or different volumes on a single router.

   c. **Click on Add.**

   The selected routers appear in the Current Routers list followed by the volume (Figure 5-11).

   In Figure 5-11, you will transfer the same files to volume 3 on two different routers in the Current Routers list.



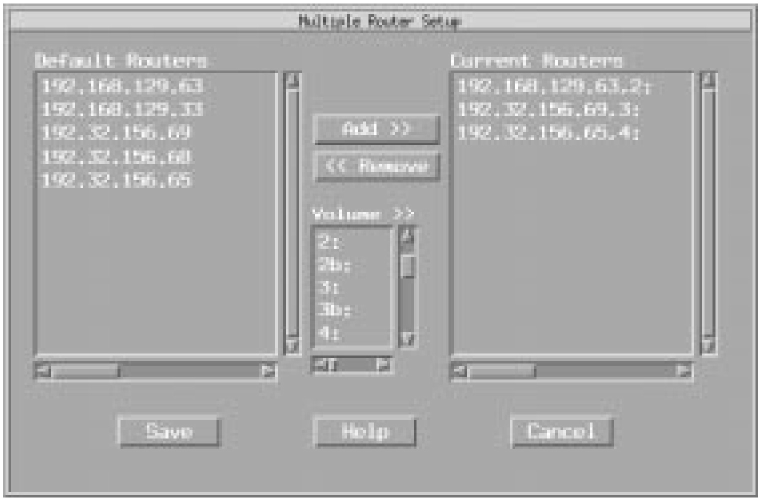
Default Routers:
192.168.129.63
192.168.129.33
192.32.156.69
192.32.156.68
192.32.156.65

Volume:
1:
1b:
2:
2b:
3:

Current Routers:
192.168.129.63.3:
192.168.129.33.3:

Figure 5-11. Adding Routers to the Current Routers List

In Figure 5-12, you will transfer the same files to volume 2 on the first router, volume 3 on the second router, and volume 4 on the third router.



Default Routers:

192.168.129.63
192.168.129.33
192.32.156.69
192.32.156.68
192.32.156.65

Current Routers:

192.168.129.63.2;
192.32.156.69.3;
192.32.156.65.4;

Volume:

2:
2b:
3:
3b:
4:

Figure 5-12. Multiple Volumes and Routers in the Router Setup Window

To remove an entry from the Current Routers list, select the router entry and click on Remove.

5. **Click on Save.**

6. **Go to "Using the Put Files Option to Transfer Files" on page 5-19.**

Using the Put Files Option to Transfer Files

To transfer files to one or more routers:

1. **In the Router Files Manager window, choose Options > Router Connection and specify the IP address of the destination router.**

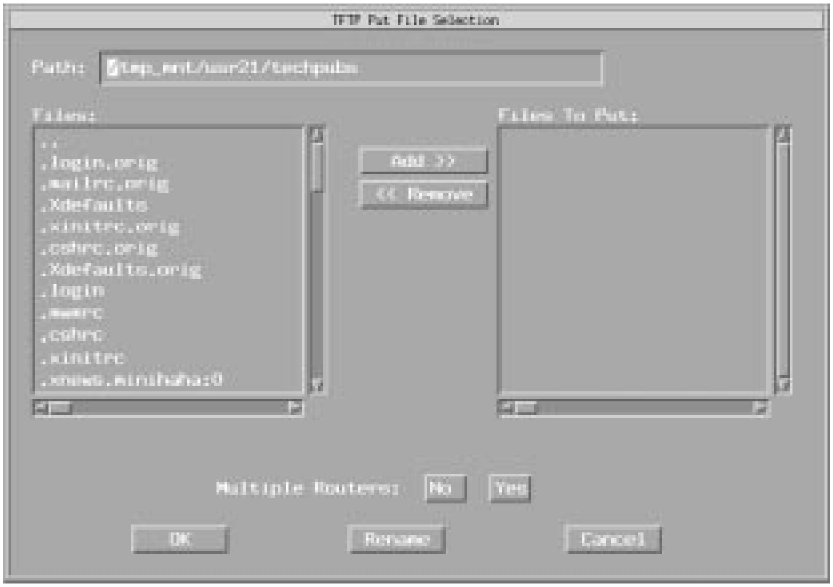
2. **Click on OK.**

   To transfer files to more than one router at a time, follow the instructions in "Setting Up File Transfers to Multiple Routers" on page 5-17.

3. **Select a router volume in the Volume field at the top of the window.**

4. **Choose File > TFTP > Put File(s).**

   The TFTP Put File Selection window opens (Figure 5-13).



Path: /tmp_mnt/usr21/techpubs

```
..
.login.orig
.mailrc.orig
.Xdefaults
.xinitrc.orig
.cshrc.orig
.Xdefaults.orig
.login
.mwmrc
.cshrc
.xinitrc
.xnews.minihaha:0
```

Figure 5-13. TFTP Put File Selection Window

5. **In the Path field, type the path to the directory on the Site Manager workstation that contains the files you want to transfer.**

   The files in that directory appear in the Files list.

6. **In the Files list, click on the files that you want to transfer.**

7. **Click on Add.**

   The selected files appear in the Files To Put list.

   If you inadvertently add files that you do not want to transfer, select those files in the Files To Put list and click on Remove.

8. **Repeat steps 4 through 6 to select files from other directories that you want to transfer.**

9. **Click on No in the Multiple Routers field to send files to only one router. Click on Yes to send files to multiple routers.**

10. **Click on OK to transfer the files under the same name, or go to step 11 to transfer the files under a new name.**

    The Router Files Manager transfers the files to the router. If a file of the same name is already in that directory, the transferred file overwrites it.

11. **To transfer a file under a new name, click on Rename.**

    The TFTP Rename Files window opens (Figure 5-14).

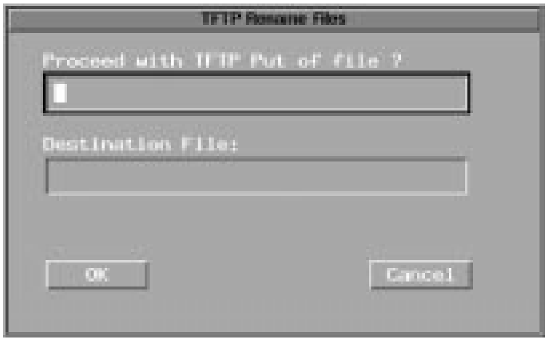


Figure 5-14. TFTP Rename Files Window

a. **Enter the name of the file you want to transfer to the router in the Proceed with TFTP Put of file field.**

b. **Enter the new file name in the Destination File field.**

c. **Click on OK.**

   The Router Files Manager transfers the file to the router under the new name. You then return to the TFTP Put File Selection window.

Note: You can transfer a renamed file to only one router at a time (the router to which you are currently connected), even if you choose multiple routers in the TFTP Put File Selection window.

Backing Up Router Software Files to a Host Computer

Bay Networks recommends that you use TFTP to back up the contents of flash memory 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 and are distributed only as backups for the boot EEPROMs.

Refer to “Copying a File” on page 5-8 for instructions.

Compacting Flash Memory

When you delete a file from flash memory, the file becomes inaccessible, but the data remains in memory, taking up space. To provide more file space and to ensure that the available free space is contiguous, you must compact memory.

Use the Router Files Manager Compact option to copy the active files from the flash memory card to the router’s memory, erase the flash memory card, and copy the files back to the memory card.

Before you use the Compact option, be sure to do the following:

- Back up the files by copying them to a second memory card.
- Compact file space at off-peak hours if possible, due to the resource requirements for performing the compaction.

The instructions that follow apply to flash memory cards and flash SIMMs.

To compact the flash memory:

1. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

2. **Select the volume that contains the flash memory media you want to compact.**

3. **Choose Commands > Compact.**

   A confirmation window appears.

4. **Click on OK to begin compacting.**

Caution: On AN and ANH routers, the compacting operation can take up to 12 minutes. Refrain from resetting the router during this time. Resetting the router during compacting corrupts the memory card, and the router will not boot until you replace the memory card.

While the operation is in progress, a running percentage of work completed appears next to the Volume field in the Router Files Manager window. After the flash memory is compacted, the Router Files Manager displays the list of files stored on the flash media.

The router is unavailable for any other file system requests until it finishes compacting. If you issue a file system request before the router finishes compacting memory, you see the following message:

```
Last command failed appears.
```

This messages indicates that the router did not successfully complete the operation. You will have to repeat the procedure.

Caution: While the router is compacting memory, 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. Likewise, if you remove a memory card while it is being compacted, the memory card can become corrupted and lose its stored data.

Formatting Flash Memory

The Router Files Manager Format option allows you to format and initialize flash memory. Use the Format option to format new memory cards or SIMMs, if you did not obtain them from Bay Networks.

Caution: You cannot recover files after you use the Format option. Copy all files to a second memory card or SIMM before you use the Format option.

The instructions that follow apply to flash memory cards and flash SIMMs.

To format a memory card:

1. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

2. **Select the volume that contains the memory media you want to format.**
3. **Choose Commands > Format.**

   A confirmation window appears.

4. **Click on OK.**

   The router formats and initializes the memory.

5. **Display a list of the volume's contents when the format operation is done.**

   Formatting is complete if the Router Files Manager does not display any files.

Partitioning Media on AN, ANH, and ASN Routers

The AN, ANH, and ASN 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 flash SIMM; the BayStack AN, ANH, and ASN use a flash memory card. If the single flash file system fails, the router has no backup file system from which to boot.

Site Manager allows you to partition the flash media on these routers. You can partition file systems on 4 MB, 8 MB, and 16 MB media only.

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 the router is unable to boot from the primary file system, it automatically attempts to boot from the secondary (backup) file system.

For example, suppose the file system for your AN 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.

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.

The next two sections explain how to create a partition and how to delete one.

Creating a Partition

To partition the NVFS:

1. **In the main Site Manager window, choose Tools > Router Files Manager.**

   The Router Files Manager window opens (refer to Figure 5-1).

2. **Select the volume you want to partition.**

   Make sure the value for `Contiguous free space` is more than half the volume's total size.

   To create volumes of equal size, the existing file system cannot be more than half 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:

   -- Delete some files, as described in "Deleting a File" on page 5-10.

   -- Compact the files, as described in "Compacting Flash Memory" on page 5-22.

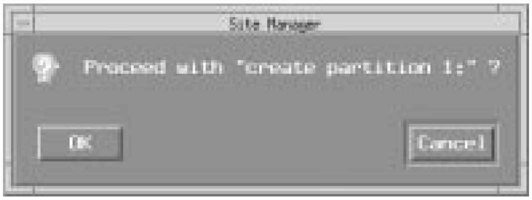
   -- Format the media, as described in the previous section.

3. **Make sure that the flash memory card is not write-protected.**

   Bay Networks ships memory cards unprotected. Refer to the installation guide for the BayStack AN, ANH, or ASN for information about setting the Read/Write switch on the flash memory card.

4. **Choose Commands > Create Partition.**

   A window opens asking you to confirm your decision to partition the media (Figure 5-15).



Proceed with "create partition 1:" ?

Figure 5-15. Create Partition Confirmation Window

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

Site Manager displays the following message next to the Volume field in the Router Files Manager window:

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

When the process is complete, the following message appears:

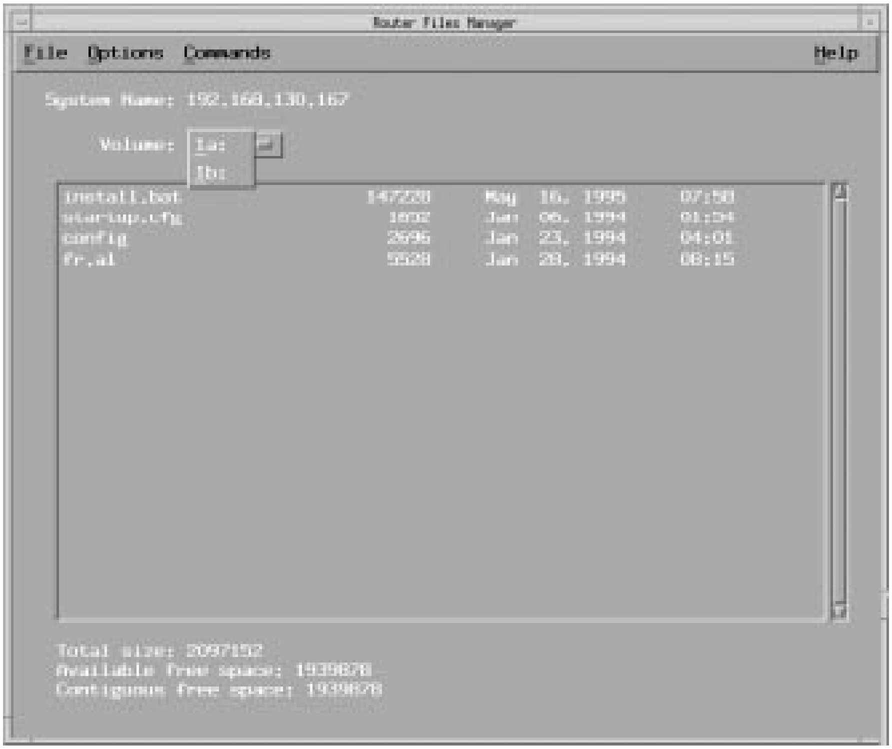
```
Media partition created. Issuing DIRECTORY command.
```

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

<*slot*><*volume*>:

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 and ANH, 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. (Refer to the ASN installation manual for information about setting the slot ID.) For example, if you partition an AN router's file system, Site Manager refers to the primary volume as **1a** and the secondary volume as **1b** (Figure 5-16).



```
System Name: 192.168.130.167

     Volume: 1a:
             1b:

install.bat                147228    May  16, 1995    07:58
startup.cfg                  1032    Jan  06, 1994    01:34
config                       2696    Jan  23, 1994    04:01
fr.al                        5528    Jan  28, 1994    08:15

Total size: 2097152
Available free space: 1939878
Contiguous free space: 1939878
```

Figure 5-16. Volume Identifiers for Partitioned Media

To manage the files on a partitioned volume, you can use any command that you would 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 the Router Files Manager Command > Copy option to copy the router files to the new volume. Refer to “Copying a File” on page 5-8.

➡ **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 on the secondary volume only.

Deleting a Partition

If you partitioned the NVFS, 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 the total media size.

Caution: 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 media.

To delete a partition:

1. **In the Router Files Manager window, click on the Volume field and switch to the primary volume.**
2. **Choose Commands > Delete Partition.**

   A window opens asking you to confirm your decision to delete the partition.
3. **Click on OK in the confirmation window.**

   Site Manager displays the following message next to the Volume field 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
Customizing Router Software Images

You can customize the router’s software image using a Site Manager tool called the Image Builder. In most cases, you use the Image Builder when you are upgrading the router with new software; however, you can use it to change the software image currently operating on a router.

The Image Builder lets you customize a software image in the following ways:

- Remove a protocol that you do not use.

  You might want to remove protocols to make more space available on the media that contains the router software image.

- Add a protocol that you removed inadvertently.
- Upgrade your router by replacing an existing image with a new one.
- Consolidate the software image.

  Sometimes Bay Networks supplies the software image on two diskettes. You might want to consolidate the two parts into one image.

- View information about the image components.

  The Image Builder displays a router software image as a list of individual components.

- Convert an image you created to an equivalent image for a different type of router.
- Create an entirely new software image.

  You can make an entirely new image from several custom images.

The chapter contains the following information:

Note: If you are upgrading your software, you should have already ordered new software from Bay Networks and received a CD. If you have a router that uses diskettes, contact the Bay Networks Technical Solutions Center for instructions about upgrading router software.

Overview of Router Software Images

A router software image is a group of executable files that contain a version of the router software for a router. You modify an image file to update or change the software. The type of software image a router uses depends on the type of router.

Table 6-1 lists router software images by router type.

Table 6-1. Router Software Image Types

Router	Software Image	Device Where Image Resides
AN	an.exe	Flash card
AFN (flash)	afn.exe	Flash card
ANH	an.exe	Flash card
ARE	bn.exe	Flash card
ARN	arn.exe	Flash card
ASN	asn.exe	Flash card
BCN®	bn.exe	Flash card
BLN	bn.exe	Flash card
CN, FN, LN (VME)	ace.out	Flash card
IN	in.exe	Flash card
5380, 5580, 5780	s5000.exe	Flash card
5780 ARE	s5000.exe	Flash card

The image contains all executable files for the current router software. Most executable files have an extension of *.exe*. The exceptions are protocol files on the CN, FN, and LN routers, which use the extension *.out*, the ATM Routing Engine (ARE) slots, which use the extension *.ppc*. The *.ppc* files are equivalent to *.exe* files. For example, instead of using *ip.exe* on an ARE slot, the router uses *ip.ppc*.

Image Builder Tool

The Image Builder lets you determine the files in a software image and modify the image contents. When you select the Image Builder from the Tools menu, the Image Builder window opens (Figure 6-1).

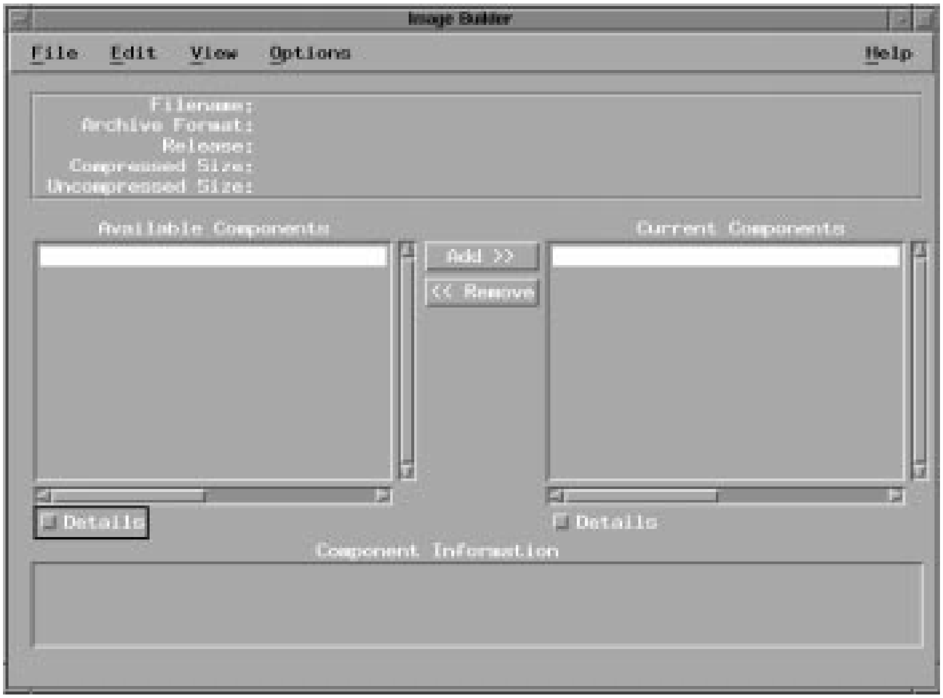


Figure 6-1. Image Builder Window

The following sections describe the main Image Builder window.

The Image Builder Menu Bar

The Image Builder menu bar consists of the following options:

File -- Lets you open, close, and save files, change the format and the release of the image, and exit the Image Builder.

Edit -- Lets you add and remove components from an image, and includes the Undo, and Redo options, which let you cancel your last action or redo your last cancelled action.

View -- Lets you view details about the available and current components.

Options -- Lets you create a text file of the software image.

Image Information

The top part of the window lists information about the software image, such as the file name, the format it was saved in, the software version of the image, and its compressed and uncompressed size.

Available Components and Current Components Lists

The software image consists of *components*. A component is a collection of files that make up a protocol or software feature. The component file is included in the executable image file, for example, *bn.exe*.

The Available Components list contains all the software components that are available as part of the router software image. This list does not reflect what a router is currently using as its software image.

The Current Components list includes the subset of components that make up the router’s software image from the complete set of image components.

You can scroll through both lists to see the complete list.

Details Buttons

The Details button is below the Available Components and Current Components lists. You can click on Details to display all the executable files that make up a list of components. To return to the list of components, click on Details again.

For example, if you click on Details for current components, all the components in that list open to reveal the executable files that make up those components. Protocol components may contain only a few files, whereas the baseline router software component contains many files, including the operating system kernel.

You can also choose the View option from the menu bar to display details about a list of components.

Component Information Box

At the bottom of the Image Builder window is the Component Information box, which lists details about a selected component (refer to Figure 6-1). When you select a component from the Available Components or Current Components list, the Image Builder displays the following information in this box:

- Order number and name of the component
- Router software version
- Compressed size of the files
- Uncompressed size of the files

The Image Builder uses an asterisk (*) to denote a partial component. A partial component is a component from which you removed a file.

Loading Image Files into the Image Builder

To upgrade an image file, you should have ordered new software from Bay Networks. The software resides on a CD. To modify an existing image file, the files should already reside on your Site Manager workstation.

You can load software into the Image Builder from CD, network directory, or any other location where the files reside. When you open the image file using the Image Builder, Site Manager copies the image to the Image Builder directory.

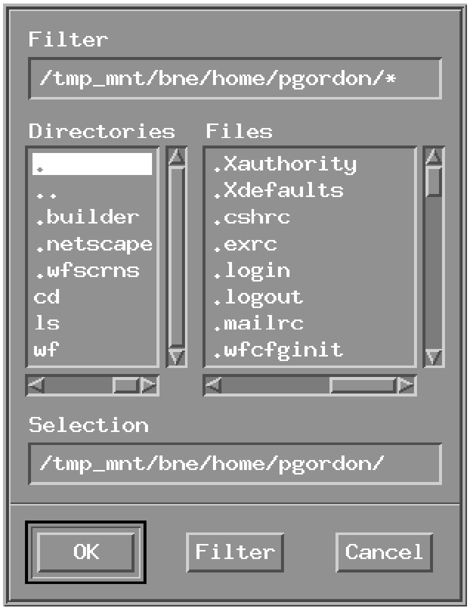
To load the software into the Image Builder:

1. **In the main Site Manager window, choose Tools > Image Builder.**

   The Image Builder window opens (refer to Figure 6-1).

2. **Choose File > Open.**

   The window in Figure 6-2 opens listing directories and files.



Filter
/tmp_mnt/bne/home/pgordon/*

Directories
.
..
.builder
.netscape
.wfscrns
cd
ls
wf

Files
.Xauthority
.Xdefaults
.cshrc
.exrc
.login
.logout
.mailrc
.wfcfginit

Selection
/tmp_mnt/bne/home/pgordon/

Figure 6-2. Open Window

3. **Go to the directory where the image files reside.**

   If you are loading files from a CD that you received from Bay Networks, the files are in the following default directories:

   - For the PC: *rtr_xxxx*, for example, *rtr_1200*
   - For UNIX: */cdrom/release_xxxx/yyy*, for example, */cdrom/release_1200_600*

4. **Double-click on the directory that contains the image you want to load.**

5. **Select the file name of the image that you want to open.**

   The directory and file name that you specify depend on the following:

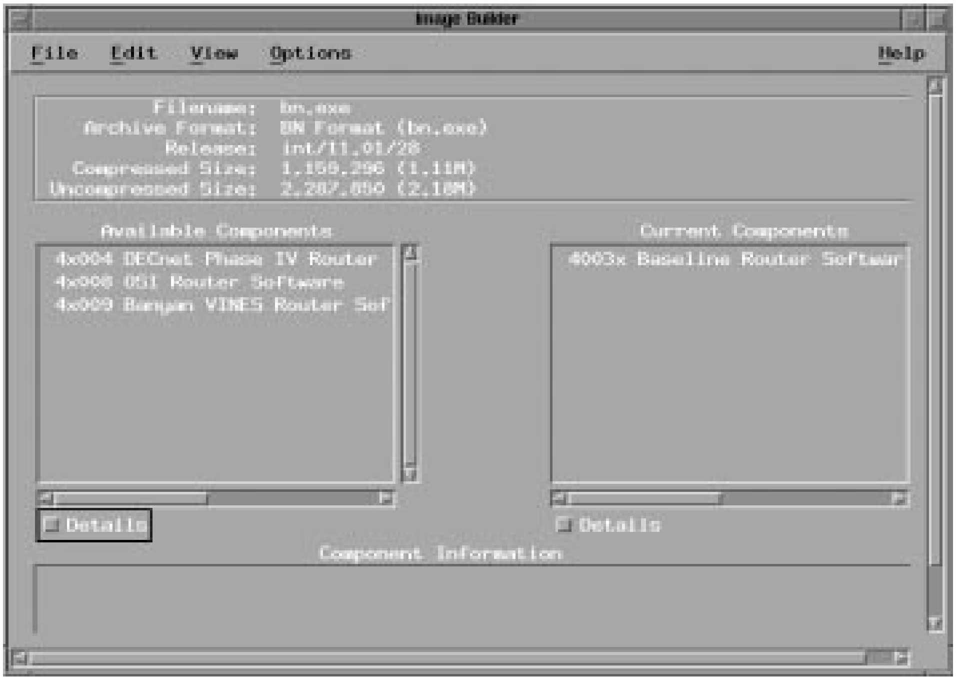
   - The computer platform (UNIX workstation or PC)
   - The type of router platform (VME or ACE)

   If you loaded the router software onto a UNIX workstation, the system stored the image in the associated directory for that router. For example, the image *bn.exe* for the VME platform is in the *vme* directory.

   If you loaded the router software onto a PC, the system stored the router image in the directory that you created for the image, for example, *\wf\xxx*.

6. **Click on OK.**

   After you select the directory and file name of the image, the Image Builder window lists the current components of the image (Figure 6-3). The components listed vary depending on the version of software you are using.



Filename: bn.exe
Archive Format: BN Format (bn.exe)
Release: int/11.01/28
Compressed Size: 1,159,296 (1.11M)
Uncompressed Size: 2,287,850 (2.18M)

Available Components

4x004 DECnet Phase IV Router
4x008 OSI Router Software
4x009 Banyan VINES Router Sof

Current Components

4003x Baseline Router Softwar

Figure 6-3. Image Builder Window with Current Components

7. **Go to "Using the Image Builder to Modify the Software Image " on page 6-10.**

Using the Image Builder to Modify the Software Image

When you use the Image Builder, it creates a builder directory. On a PC, the directory is *\wf\builder.dir.* On a UNIX workstation, the directory is defined by the environment variable BUILDER_DIR. You should have already defined this variable during the Quick-Start procedure (refer to *Quick-Starting Routers* for instructions).

This directory may contain portions of old images that are no longer in use, unless this is a new installation. You can remove these partial images to free up space on your PC or UNIX workstation.

Be sure you have enough space on the destination router volume to transfer the new or modified image to the router. To check the available space, refer to Chapter 5 for instructions.

Removing Software Components

You can remove files from the software image to make more space available on the router software volume.

The Image Builder will not let you remove essential files. This protects the most important files that make up your router software image. For example, you cannot remove the Operating System Kernel file from the baseline router software component. Also, because the baseline router software component contains essential files, you cannot remove it from the list of current components.

To remove components from the software image:

1. **In the main Site Manager window, choose Tools > Image Builder.**

   The Image Builder window opens (refer to Figure 6-1).

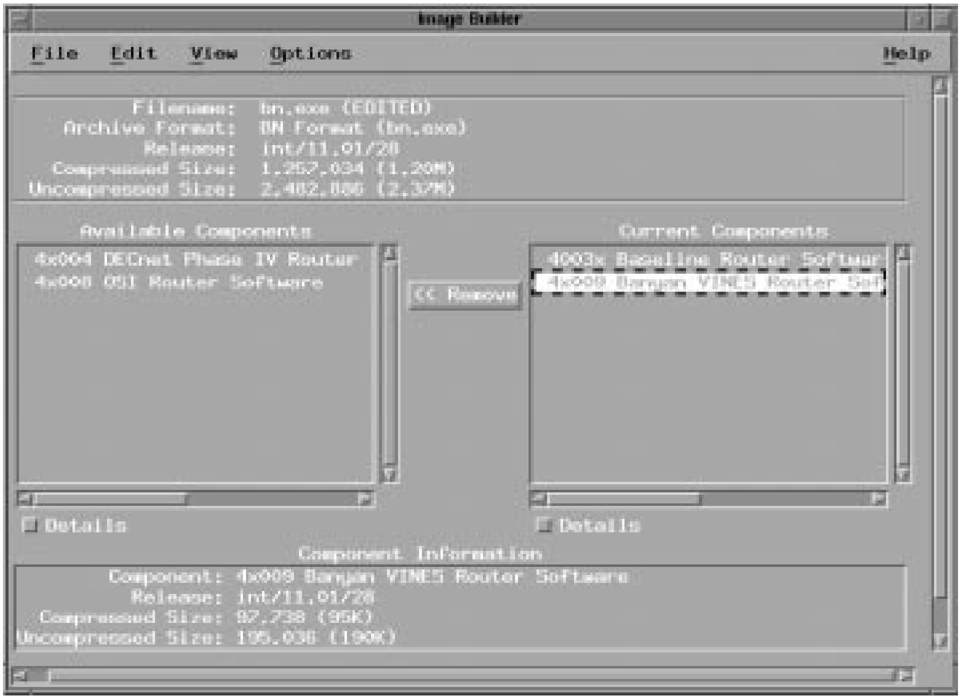
2. **Load the router software into the Image Builder.**

   Refer to "Loading Image Files into the Image Builder" on page 6-7.

3. **Select the file in the Current Components list that you want to remove.**

   The Remove button appears in the Image Builder window (Figure 6-4).

   If you select an essential file that you should not remove, for example, the Operating System Kernel file from the baseline router software component, you will not see the Remove button.



```
          Filename:  bn.exe (EDITED)
    Archive Format:  BN Format (bn.exe)
           Release:  int/11.01/28
   Compressed Size:  1,257,034 (1.20M)
 Uncompressed Size:  2,482,886 (2.37M)
```

Available Components
- 4x004 DECnet Phase IV Router
- 4x008 OSI Router Software

Current Components
- 4003x Baseline Router Softwar
- 4x009 Banyan VINES Router Sof

Component Information

```
        Component: 4x009 Banyan VINES Router Software
          Release: int/11.01/28
  Compressed Size: 97,738 (95K)
Uncompressed Size: 195,036 (190K)
```

Figure 6-4. Image Builder Window with the Remove Button

4. **Click on Remove.**

   The Image Builder removes the component from the Current Components list and moves it to the Available Components list.

   You can also choose Edit > Remove Component from the Image Builder menu bar to remove a component. To remove all components from the image, choose Edit > Remove All Components. You do not need to select each component individually before you choose this option.

5. **Go to "Saving a Modified Image" on page 6-14.**

Adding Software Components

If you removed files from an existing software image, or you changed the router's hardware modules to add functionality, you may want to add components to the software image.

To add a component to the software image:

1. **In the main Site Manager window, choose Tools > Image Builder.**

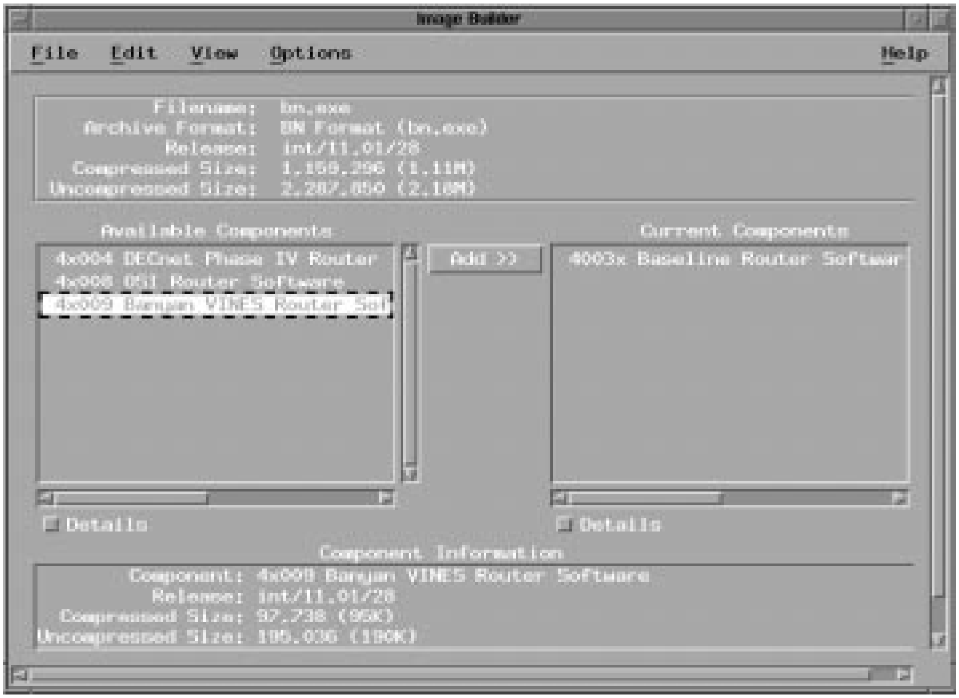
   The Image Builder window opens (refer to Figure 6-1).

2. **Load the router software into the Image Builder.**

   Refer to "Loading Image Files into the Image Builder" on page 6-7.

3. **Select the file in the Available Components list that you want to add.**

   The Add button appears in the Image Builder window (Figure 6-5).



```
        Filename:  bn.exe
  Archive Format:  BN Format (bn.exe)
         Release:  int/11.01/28
 Compressed Size:  1,159,296 (1.11M)
Uncompressed Size: 2,287,850 (2.18M)
```

Available Components
- 4x004 DECnet Phase IV Router
- 4x008 OSI Router Software
- 4x009 Banyan VINES Router Sof

Current Components
- 4003x Baseline Router Softwar

Component Information

```
        Component: 4x009 Banyan VINES Router Software
          Release: int/11.01/28
  Compressed Size: 97,738 (95K)
Uncompressed Size: 195,036 (190K)
```

Figure 6-5. Image Builder Window with the Add Button

4. **Click on Add.**

   The component moves from the Available Components list to the Current Components list.

   You can also add components by choosing Edit > Add from the Image Builder menu bar. To add all components that appear in the Available Components list, choose Edit > Add All Components. You do not need to select each component individually before you choose this option.

Note: In Figure 6-4, the word EDITED appears in parentheses next to the Filename field. This word is displayed whenever you load a previously modified file into the Image Builder.

5. **Go to "Saving a Modified Image" on page 6-14.**

Saving a Modified Image

The Image Builder automatically archives all software images in the Image Builder directory, which is created when you install Site Manager. (Refer to *Quick-Starting Routers* for information about installing Site Manager.) The Image Builder saves only individual components in this directory, which are listed in the Available Components list. Bay Networks recommends that you save modified software images in a different directory.

If you save files locally on the Site Manager workstation, use different image file names for each router on your network and keep a record of which images are operating on which routers.

You may want to save the image in the same directory in which you loaded the router software. (Refer to "Loading Image Files into the Image Builder" on page 6-7.) Be sure that you include all components you want before you save the image.

To save the modified image:

1. **In the Image Builder window, choose File > Save.**

   This saves the image to your current directory. There is no confirmation window after the image is saved successfully.

2. **To save a second copy of the image under another name, choose File > Save As.**

   The Save As window opens. This window is similar to Figure 6-2.

3. **Select a directory from the Directories scroll list.**
4. **Type a file name in the Selection field.**
5. **Click on OK.**

   The new image is saved and the updated file name, version, compressed and uncompressed file size appear at the top of the Image Builder window (refer to Figure 6-5).

   If you are copying the new image to a diskette, refer to the compressed and uncompressed size of the image to determine whether it will fit on a diskette.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

If you exit the Image Builder without saving your changes, you are asked if the changes should be discarded before you exit.

7. **Transfer the new image to the router using the Router Files Manager.**

    The Router Files Manager lets you transfer files between the Site Manager workstation and any Bay Networks router using TFTP.

    If space is available, you should keep the old software image on the router until you succeed in booting it with the new image. If space is not available, delete the old image and then transfer the new one. Refer to Chapter 5 for instructions.

➡ **Note:** Be sure that all the files in the image are from the same router software version.

8. **Use a named boot and boot the router with the new image.**

    Refer to Chapter 4 for instructions on performing a named boot.

    If the router has the available memory, test the new image file before you overwrite the existing image.

Creating a New Image

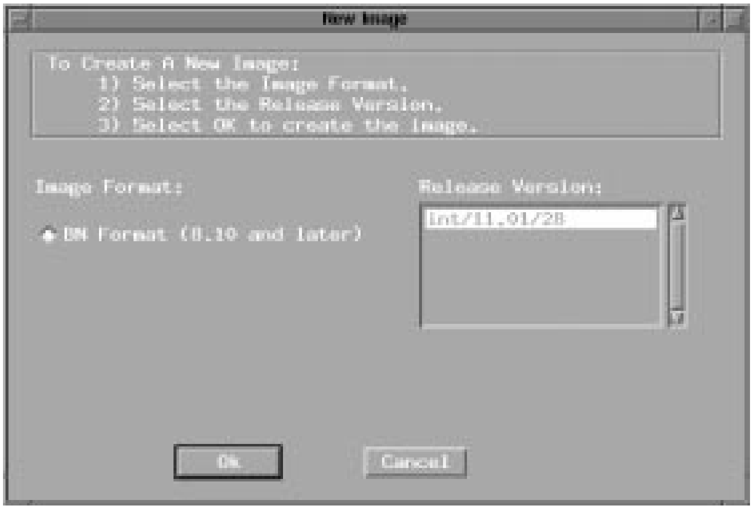
Creating an entirely new image is usually not necessary; however, the Image Builder provides the option if you need it. For example, you might want to completely reconfigure the router's software image or perform a major upgrade from a very old version of software to the most current version.

To create a new image:

1. **In the Image Builder window, choose File > New.**

   The New Image window opens (Figure 6-6).

   You cannot choose the New command unless the router software files are archived in the Image Builder directory.



```
To Create A New Image:
    1) Select the Image Format.
    2) Select the Release Version.
    3) Select OK to create the image.
```

Image Format:

● BN Format (8.10 and later)

Release Version:

int/11.01/28

Figure 6-6. New Image Window

2. **Confirm that the format you want is available.**

   The image formats that appear in the New Image window are those that you loaded into the Image Builder. For example, the image *bn.exe* is in the Image Builder, which is why you can select the BN/BNX format.

   If you cannot select the image format you want, you need to load the image associated with the image format into the Image Builder. Refer to "Loading Image Files into the Image Builder" on page 6-7 for instructions.

3. **Select the appropriate image format, then click on OK.**

   An empty Image Builder window opens.

   You can now build a new image using the router software on your workstation. Refer to "Using the Image Builder to Modify the Software Image" on page 6-10 for instructions.

Converting an Image for Other Types of Routers

If you want to run the same image on different types of Bay Networks routers in a network, you can create an image for one type of router and convert the image to run on other types of routers. For example, you might want to run the same protocols on AN and BN routers in a network. You can customize an image for the BN routers and then convert that image to run on the AN routers.

You can use this feature only to convert to image formats that you previously loaded into the Image Builder.

To convert an image for a different router type:

1. **In the Image Builder window, choose File > Change Format.**

   A window with a list of image formats opens (refer to Figure 6-6).

2. **Confirm that the format you want is available.**

   If you cannot select the image format you want because it is dimmed, you need to load the image associated with that image format into the Image Builder. Refer to "Loading Image Files into the Image Builder" on page 6-7 for instructions.

3. **Select a format from the list.**

   The image changes to the format you selected.

4. **Save the modified image.**

   Refer to "Saving a Modified Image" on page 6-14 for instructions.

Converting an Image for Other Software Versions

You may have Bay Networks routers in a network that use different versions of router software. To run the same image on all routers, you can create an image for a router running one software version and convert the image for routers running other software versions.

For example, you might want to run the same image on routers running Version 11.00 software and routers running Version 12.00 software. You can create an image with Version 12.00 files and convert the image to use with Version 11.00 files.

You can use this feature only to convert images to software versions that you previously loaded into the Image Builder.

To convert an image to a different software version:

1. **In the Image Builder window, choose File > Change Release.**

   A list of software versions opens.

2. **Confirm that the release version you want is available.**

   If you cannot select the version you want, you need to load the associated image for that version into the Image Builder. Refer to “Loading Image Files into the Image Builder” on page 6-7 for instructions.

3. **Select a version from the list.**

   The image changes to the software version you selected.

4. **Save the modified image.**

   Refer to “Saving a Modified Image” on page 6-14.

Saving the Contents of the Current Component List to a File

To keep a record of the files included in the router's software image, you can save the Image Builder's Current Components list to an ASCII file. The *CONTENTS.TXT* file lists all the order numbers, components, file names, and descriptions shown in the Current Components list.

In the Image Builder window, save the Current Components list by choosing Options > Generate CONTENTS.TXT when Saving.

You will not see a confirmation window after selecting the option. The Image Builder creates an ASCII file named *CONTENTS.TXT* when you save an image by choosing File > Save or File > Save As.

CONTENTS.TXT is saved in the same directory as the image.

➡ **Note:** If you do not specify a directory, by default the image and the *CONTENTS.TXT* file are saved to the Image Builder directory.

Chapter 7
Monitoring Trap and Event Messages

To manage your Bay Networks routers and ensure that they are working properly, you can use trap and event messages.

Trap messages provide real-time information about the operating status of the routers in your network. Bay Networks routers use SNMP, an industry standard, which sends trap messages. The Trap Monitor tool lets you view these messages.

Event messages also provide information about the operating status of the routers in your network; however, event messages provide more detailed information than trap messages. The Events Manager tool lets you display event messages.

This chapter contains the following information:

Comparing Trap and Event Messages

Trap and event messages are closely related. Trap messages are a concise form of event messages. The information that generates trap messages comes from the same source as the event messages. By configuring a trap, you instruct the router to automatically send events to the router's SNMP manager.

To check how your routers are functioning, view the trap messages first; then view event messages for more detailed information about the routers' operating status.

Table 7-1 compares trap and event messages.

Table 7-1. Comparison of Trap and Event Messages

Trap Messages	Event Messages[a]
Show real-time display	Show detailed display not in real time
Display SNMP-standard messages and Bay Networks-specific messages	Display Bay Networks-specific messages
Use more router resources because they are sent across the network	Use fewer router resources because the display is viewed locally
Provide concise messages	Provide lengthier and more descriptive messages
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.
Use SNMP agent to send event messages to Trap Monitor.	Use Site Manager to get event log and load it into the Events Manager
Save messages to an ASCII file	Save messages to an ASCII file
Store messages in workstation's trap history file	Store messages in router's event log
Stamp messages with workstation's time	Stamp messages with router's time

[a] Refer to *Event Messages for Routers*, which lists the event messages and provides information about how to respond to them.

To configure traps messages, go to "Configuring Trap Messages" on page 7-3. To view event messages, go to "Monitoring Router Events" on page 7-23.

Configuring Trap Messages

There are two parts to configuring trap messages:

- Configuring the router's SNMP agent to send trap messages to the SNMP manager, which is your Site Manager workstation
- Using the Trap Monitor to view and manage trap messages

To set up the router's trap capability, go to the next section.

Configuring the Router's SNMP Agent

Every Bay Networks router incorporates an *SNMP management agent*. The agent is a software entity included with the software image on the flash card or diskette. The SNMP agent responds to commands and requests from an *SNMP manager*, that is, your Site Manager workstation. The agent then interprets the commands and performs the required task.

Before using the Trap Monitor, you must configure the SNMP agent on the router. After you set up the agent, you specify the types of trap messages you want to collect, then use the Trap Monitor to view and manage the messages.

You must configure the SNMP agent on the router to:

- Identify your Site Manager workstation as an SNMP manager.
- Send specified trap messages to your Site Manager workstation.

To configure the SNMP agent, use the Configuration Manager.

For more information about SNMP, refer to *Configuring SNMP, RMON, BootP, DHCP, and RARP Services*.

Identifying the Site Manager Workstation as an SNMP Manager

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

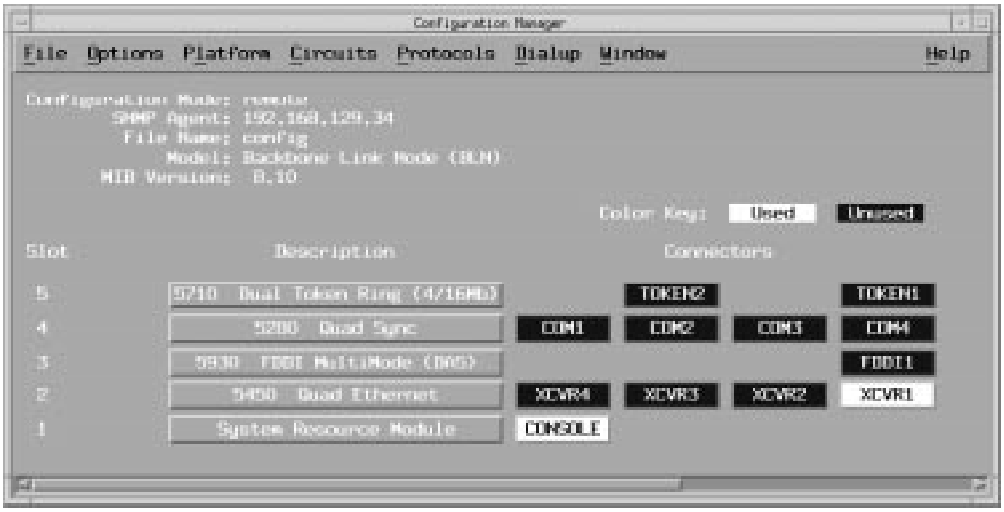
To set up the workstation as an SNMP manager:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the Site Manager window, choose Tools > Configuration Manager > Local File, Remote File, or Dynamic.**

   The Configuration Manager window opens (Figure 7-1).



```
Configuration Mode: remote
        SNMP Agent: 192.168.129.34
         File Name: config
             Model: Backbone Link Node (BLN)
      MIB Version:  8.10
```

Color Key: Used Unused

Slot	Description	Connectors			
5	5710 Dual Token Ring (4/16Mb)		TOKEN2		TOKEN1
4	5280 Quad Sync	COM1	COM2	COM3	COM4
3	5930 FDDI MultiMode (DAS)				FDDI1
2	5450 Quad Ethernet	XCVR4	XCVR3	XCVR2	XCVR1
1	System Resource Module	CONSOLE			

Figure 7-1. Configuration Manager Window

3. **Choose Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens (Figure 7-2). The default community, public, is selected.

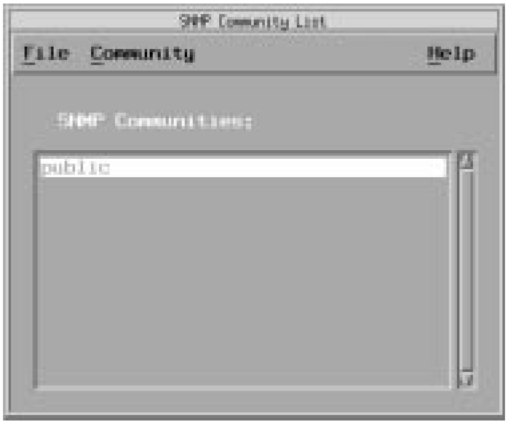


Figure 7-2. SNMP Community List Window

4. **Choose Community > Managers.**

   The SNMP Manager List window opens (Figure 7-3).

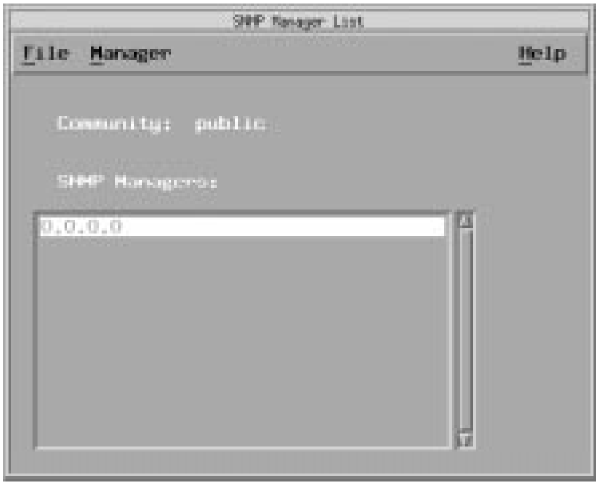


Figure 7-3. SNMP Manager List Window

5. **Choose Manager > Add Manager.**

   The Add SNMP Manager window opens (Figure 7-4).

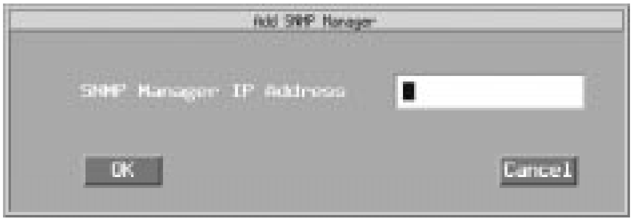


Figure 7-4. Add SNMP Manager Window

6. **Type the IP address of your Site Manager workstation, then click on OK.**

   You return to the SNMP Manager List window, which now displays your workstation's IP address.

7. **Choose File > Exit.**

   You return to the SNMP Community List window.

8. **Choose File > Exit.**

   You return to the Configuration Manager window.

9. **Choose File > Save or File > Save As to save the configuration file.**

   Specify the router volume and configuration file name. If you want this to be the default configuration, name the file *config*.

   Refer to Chapter 3 for details about saving configuration files.

Selecting Trap Messages

You can configure the SNMP agent to send trap messages to the Trap Monitor based on the following criteria:

- By category (all, generic, specific, none)

  The category determines the type of the trap messages you want to collect.

- By protocol entity

  The protocol entity instructs the agent to send trap messages for a specific protocol. You must use this criterion together with the event severity level.

- By event severity level

  The event severity level instructs the agent to send trap messages if an event with the specified severity level appears in the event log. You must use this criterion together with the protocol entity.

You can also select specific trap messages that the SNMP agent always sends or never sends, regardless of other criteria you have set. These are *trap exceptions*, and they are specified by their entity and event code.

Specifying Trap Messages by Category

You can configure the SNMP agent to send the following trap messages:

- All traps
- Generic traps
- Specific traps
- None

To specify the types of messages sent by the agent:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Communities.**

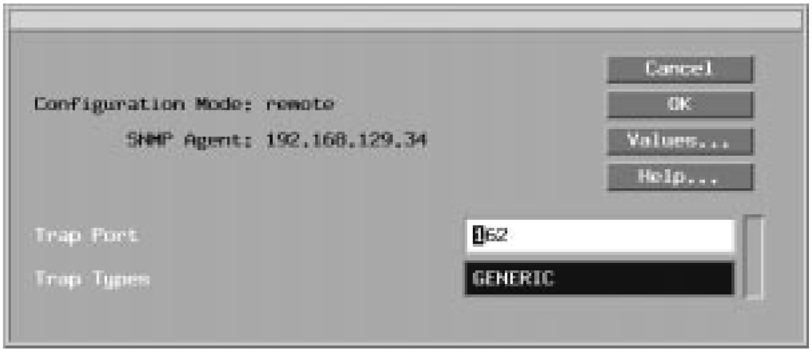
   The SNMP Community List window opens (refer to Figure 7-2).

2. **Choose Community > Managers.**

   The SNMP Manager List window opens (refer to Figure 7-3).

3. **Choose Manager > Edit Manager.**

   The Trap Port and Trap Types window opens (Figure 7-5).



Configuration Mode: remote

SNMP Agent: 192.168.129.34

Trap Port 162

Trap Types GENERIC

Figure 7-5. Trap Port and Trap Types Window

4. **Specify a value for the Trap Types parameter, then click on OK.**

   Table 7-2 lists the different trap types.

Table 7-2. Trap Types

Type[a]	**Description**
All	Instructs 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).
Generic	Instructs the agent to transmit well-defined SNMP traps (cold-start, warm-start, and authentication failure traps). The agent is automatically enabled to send cold-start and warm-start traps. To transmit authentication failure trap messages, you must enable the Authentication Failure Trap parameter. Refer to *Configuring SNMP, RMON, BootP, DHCP, and RARP Services* for instructions.
Specific	Instructs the agent to send only trap messages for a specific protocol entity and event severity level (fault, warning, debug, information, and trace). Refer to "Specifying Trap Messages by Protocol Entity and Event Severity" for instructions.
None	Prohibits the SNMP agent from transmitting traps to the SNMP manager.

[a] Specifying generic or specific trap messages minimizes the agent's use of router resources.

After you select a trap type, you return to the Configuration Manager window.

5. **Choose File > Save to save the configuration file.**

   Refer to Chapter 3 for more instructions on saving configuration files.

Specifying Trap Messages by Protocol Entity and Event Severity

If you configure an SNMP manager's trap type to **specific**, you instruct the SNMP agent to send trap messages based on the protocol entity and event severity level that you specify. You must specify both criteria. For example, if you select IP as the entity and Fault as the event severity, you receive only IP fault messages. If you want messages for another entity, you must specify a separate entry.

To set up specific trap messages:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Trap Configuration > Interfaces.**

   The Trap Configuration window opens (Figure 7-6).

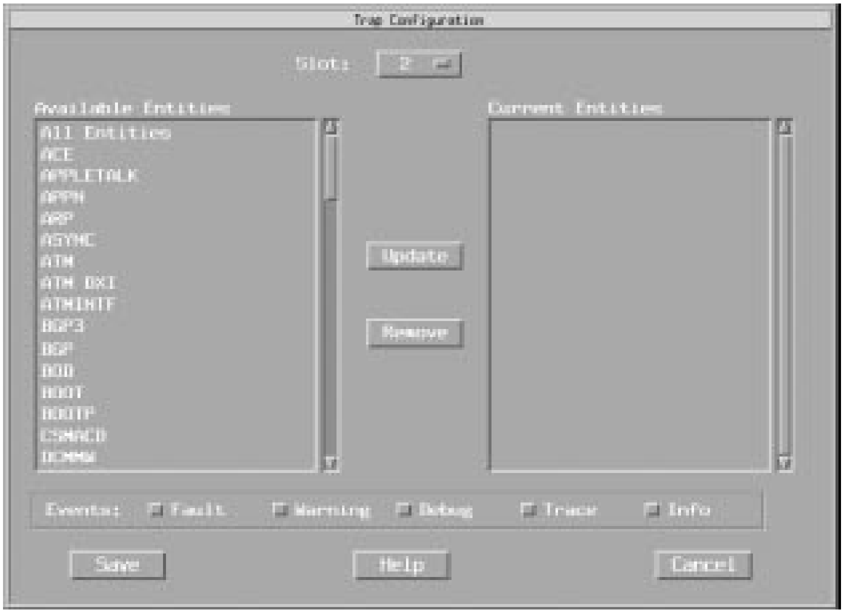


Figure 7-6. Trap Configuration Window

2. **Select the appropriate slot by clicking in the Slot field.**
3. **Select an entity from the Available Entities list.**

4. **Select the event severity from the Events field.**

   This specifies what type of event triggers a trap message for the selected entity.

5. **Click on Update.**

   The entity and event are added to the Current Entities list.

6. **Repeat steps 2 through 5 for every entity whose trap messages you want to receive.**

7. **Click on Save.**

   You return to the Configuration Manager window.

8. **Choose File > Save to save this configuration file.**

   Refer to Chapter 3 for instructions.

The entities you selected will now send the trap messages you selected to your Site Manager workstation.

Specifying Trap Message Exceptions

You can configure the router's SNMP agent to send specific trap messages all the time or not at all. You select these types of exceptions by their unique entity and event code.

To specify trap message exceptions:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Trap Configuration > Exceptions.**

   The Traps Exceptions Lists window opens (Figure 7-7).

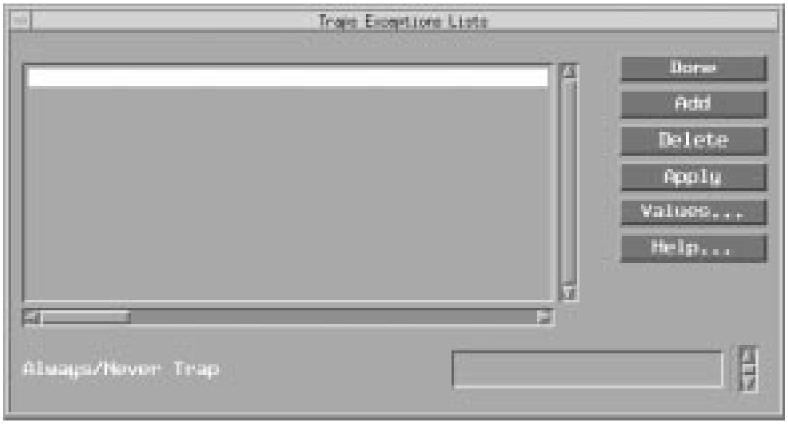
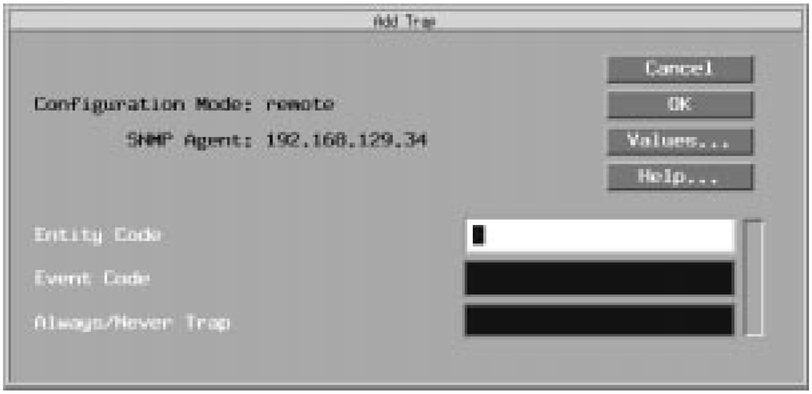


Figure 7-7. Traps Exceptions Lists Window

2. **Click on Add.**

   The Add Trap window opens (Figure 7-8).



Add Trap

Configuration Mode: remote

SNMP Agent: 192.168.129.34

Entity Code

Event Code

Always/Never Trap

Figure 7-8. Add Trap Window

3. **Type values for the parameters in the Add Trap window.**

   To determine the entity code and event code values, refer to *Event Messages for Routers.*

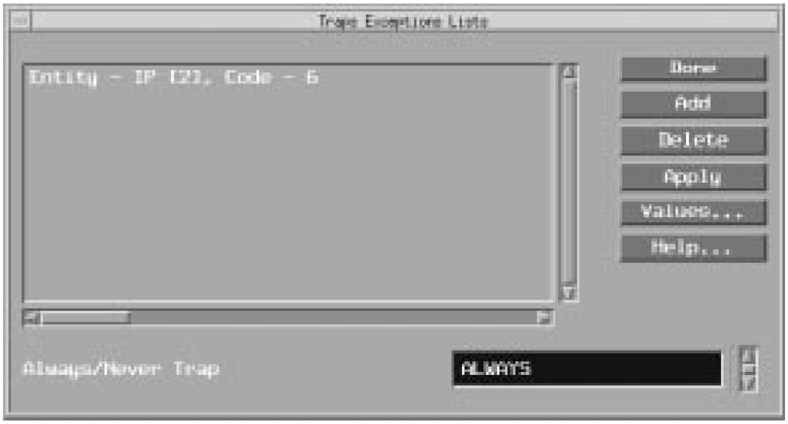
   Table 7-3 lists the options for each parameter.

Table 7-3. Entering Values in the Add Trap Window

Field	Value
Entity Code	Enter a value from 0 to 61.
Event Code	Enter a value from 0 to 255.
Always/Never Trap	Enter Always to receive this trap message; otherwise, enter Never Trap.

4. **Click on OK.**

   You return to the Traps Exceptions Lists window (Figure 7-9), which displays the trap entry.



Entity - IP [21], Code - 6

Always/Never Trap ALWAYS

Figure 7-9. Traps Exceptions Lists Window

5. **Click on Apply.**
6. **Repeat steps 2 through 5 for each trap exception you want to configure.**
7. **Click on Done.**

   You return to the Configuration Manager.

8. **Choose File > Save to save the configuration file.**

   Refer to Chapter 3 for instructions.

   You have now configured the SNMP agent for a router. The agent will now send the trap messages you specified to the Site Manager workstation.

9. **Go to "Using the Trap Monitor" on page 7-15 to view trap messages using the Trap Monitor.**

If you are running multiple network management applications, go to "Changing the Trap Port for Multiple Network Management Applications" on page 7-14.

Changing the Trap Port for Multiple Network Management Applications

If you are running more than one network management application on your Site Manager workstation, you must configure Site Manager to receive trap messages from the SNMP agent on a port other than the default port, 162. This is necessary for the following reasons:

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

  By default, the network management application on your workstation is assigned to User Datagram Protocol (UDP) port 162. This port is dedicated to receiving SNMP trap messages from the SNMP agent.

  Site Manager is the preferred network management application for receiving trap messages. To avoid any problems when running another network management application, Bay Networks recommends that you configure Site Manager to map to an alternative UDP port. This allows you to send trap messages to Site Manager directly.

To reconfigure the trap port:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Communities.**

   The SNMP Community List window that opens (refer to Figure 7-2).

2. **Choose Community > Managers.**

   The SNMP Manager List window opens (refer to Figure 7-3).

3. **Choose Manager > Edit Manager.**

   The Trap Port and Trap Types window opens (refer to Figure 7-5).

4. **Type a new port number for the Trap Port parameter, then click on OK.**

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

   You return to the Configuration Manager window.

5. **Choose File > Save to save this configuration file.**

   Refer to Chapter 3 for instructions on saving configuration files.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

7. **Restart Site Manager according to the instructions in Chapter 1.**

Using the Trap Monitor

The Trap Monitor receives trap messages from all router SNMP agents on the network. After you configure a router's SNMP agent to send trap messages to the SNMP manager, that is, the 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.

Before using the Trap Monitor, you should have already configured each router's SNMP agent to send trap messages. (Refer to "Configuring the Router's SNMP Agent" on page 7-3.) After the Site Manager workstation receives the trap messages, you can instruct the Trap Monitor to filter and display a subset of these trap messages.

If you configure your router's SNMP agent to send trap messages, it sends messages regardless of whether you are currently viewing them using the Trap Monitor.

To access the Trap Monitor, begin at the main Site Manager window and choose Tools > Trap Monitor, or click on the Traps function button below the main menu.

Use the Trap Monitor to do the following:

- Load the trap messages into the Trap Monitor.
- View trap messages.
- Filter trap messages so you can see a subset of all messages sent.
- Save trap messages 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.
- Clear the trap history file to start a new log.

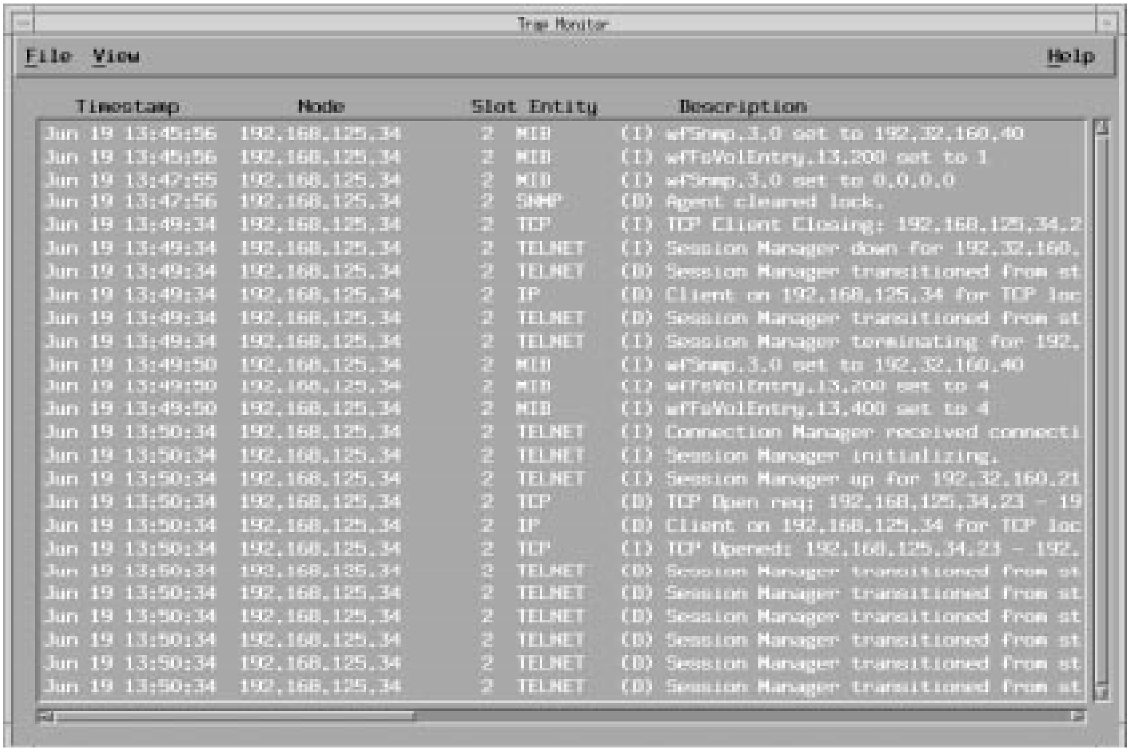
The following sections describe each of these tasks.

Loading Trap Messages into the Trap Monitor

The trap messages that Site Manager receives are stored in the trap history file. After you load the trap history file into the Trap Monitor, the Trap Monitor dynamically displays trap messages from the file.

To load trap messages, begin at the main Site Manager window and choose Tools > Trap Monitor.

The Trap Monitor window opens and displays incoming trap messages (Figure 7-10).



```
   Timestamp           Node            Slot Entity        Description
Jun 19 13:45:56  192.168.125.34         2  MIB      (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:45:56  192.168.125.34         2  MIB      (I) wfFsVolEntry.13.200 set to 1
Jun 19 13:47:55  192.168.125.34         2  MIB      (I) wfSnmp.3.0 set to 0.0.0.0
Jun 19 13:47:56  192.168.125.34         2  SNMP     (D) Agent cleared lock.
Jun 19 13:49:34  192.168.125.34         2  TCP      (I) TCP Client Closing: 192.168.125.34.2
Jun 19 13:49:34  192.168.125.34         2  TELNET   (I) Session Manager down for 192.32.160.
Jun 19 13:49:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:49:34  192.168.125.34         2  IP       (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:49:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:49:34  192.168.125.34         2  TELNET   (I) Session Manager terminating for 192.
Jun 19 13:49:50  192.168.125.34         2  MIB      (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:49:50  192.168.125.34         2  MIB      (I) wfFsVolEntry.13.200 set to 4
Jun 19 13:49:50  192.168.125.34         2  MIB      (I) wfFsVolEntry.13.400 set to 4
Jun 19 13:50:34  192.168.125.34         2  TELNET   (I) Connection Manager received connecti
Jun 19 13:50:34  192.168.125.34         2  TELNET   (I) Session Manager initializing.
Jun 19 13:50:34  192.168.125.34         2  TELNET   (I) Session Manager up for 192.32.160.21
Jun 19 13:50:34  192.168.125.34         2  TCP      (D) TCP Open req: 192.168.125.34.23 - 19
Jun 19 13:50:34  192.168.125.34         2  IP       (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:50:34  192.168.125.34         2  TCP      (I) TCP Opened: 192.168.125.34.23 - 192.
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
Jun 19 13:50:34  192.168.125.34         2  TELNET   (D) Session Manager transitioned from st
```

Figure 7-10. Trap Monitor Window

You can scroll through the trap messages using the window’s scroll bars.

Choose File > Load History File to view messages that were cleared from the previous display.

Viewing Messages in the Trap Monitor Window

The Trap Monitor menu bar contains the following options:

File -- Lets you exit the tool.

View -- Lets you view only a subset of the trap messages by type or IP address.

You view trap messages in real time using the Trap Monitor (refer to Figure 7-10). Table 7-4 describes the window contents.

Table 7-4. Trap Message Details

Column	Description
Timestamp	Displays the date and time the Site Manager workstation received the trap message
Node	Lists the IP address of the router whose SNMP agent generated the trap message
Slot	Lists the slot hosting the entity that generated the trap message
Entity	Lists the abbreviated name of the entity that generated the trap message
Severity	Lists the first letter of the trap messages' severity level: Fault, Warning, Information, Debug, or Trace. For example, W stands for Warning.
Description	Includes text describing the trap message

Viewing Specific Trap Messages

After you load the trap messages, you can filter the trap messages you view in the Trap Monitor window.

Remember that filtering the messages has no effect on which trap messages the SNMP agent sends to the Site Manager workstation. To specify the types of messages sent by the SNMP agent, refer to "Selecting Trap Messages" on page 7-7.

Using the Trap Monitor, you can filter trap messages by trap type (which is the same as the event severity level) or by IP address.

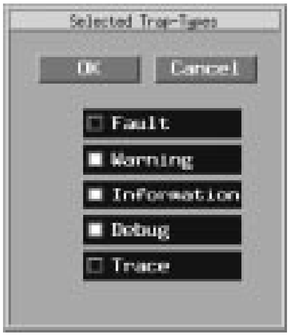
Viewing Messages by Event Severity Level

When you view trap messages by the event severity level (fault, warning, information, debug, or trace), you are seeing the trap messages triggered by a specific type of event.

To view messages by event severity:

1. **In the Trap Monitor window, choose View > Select Trap Types.**

   The Selected Trap-Types window opens (Figure 7-11).



☐ Fault
☑ Warning
☑ Information
☑ Debug
☐ Trace

Figure 7-11. Selected Trap-Types Window

2. **Select the trap types you want to see, then click on OK.**

   The Trap Monitor window displays messages of the specified types.

   To remove unwanted messages from the window, refer to “Clearing the Trap Monitor Window” on page 7-21.

3. **Choose File > Exit to exit the Trap Monitor window.**

   You return to the main Site Manager window.

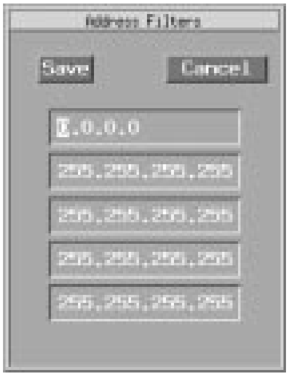
Viewing Messages by Router IP Address

Viewing messages by router IP address shows 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 agents that have the same partial IP address.

To view message by router IP address:

1. **In the Trap Monitor window, choose View > Set Address Filters.**

   The Address Filters window opens (Figure 7-12).



0.0.0.0
255.255.255.255
255.255.255.255
255.255.255.255
255.255.255.255

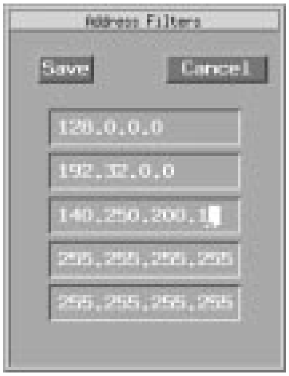
Figure 7-12. Address Filters Window

The default address filter of 0.0.0.0 instructs the Trap Monitor to display trap messages from all routers. The address filter of 255.255.255.255 is merely a placeholder for an IP address that you specify.

2. **Enter one or more complete or partial IP addresses.**

   You can enter as many as five complete or partial IP addresses. Any field that you do not fill in must display the placeholder, 255.255.255.255.

   Figure 7-13 shows an example of an Address Filters window.



128.0.0.0

192.32.0.0

140.250.200.1

255.255.255.255

255.255.255.255

Figure 7-13. Sample Address Filters Window

The window in Figure 7-13 will enable you to view trap messages from all routers with IP addresses starting with 128. and 192.32., along with those from the IP address 140.250.200.1.

3. **Click on Save.**

   After you save the filter entries, the Trap Monitor displays trap messages only from those routers with an IP address that matches the values you specified.

4. **Choose File > Exit to exit the Trap Monitor window.**

   You return to the main Site Manager window.

Saving Trap Messages

The Trap Monitor lets you save the traps currently displayed in the 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:

1. **In the Trap Monitor window, choose File > Save Traps.**

   The Trap Monitor prompts you to name the file (Figure 7-14).

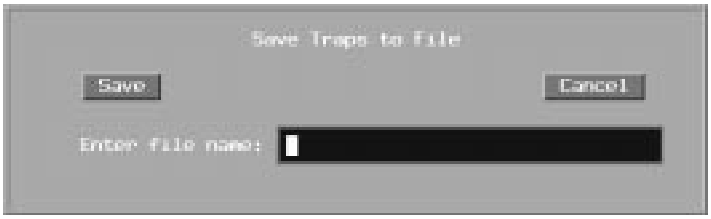


Figure 7-14. Saving Traps to a File

2. **Type a directory path and file name, then click on Save.**

   You return to the Trap Monitor window.

   The system saves the message display to an ASCII file on your computer. (If you do not specify a directory, the system saves the file to your local directory.) You cannot reload an ASCII file back into the Trap Monitor.

Clearing the Trap Monitor Window

To clear the Trap Monitor window, choose View > Clear Window. The Trap Monitor clears the window of all trap messages.

Because the SNMP agent 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 the file reaches its limit, the Trap Monitor starts overwriting the existing messages from the beginning of the file. The Trap Monitor lets you empty the current trap history file so that you can start a new list of trap messages.

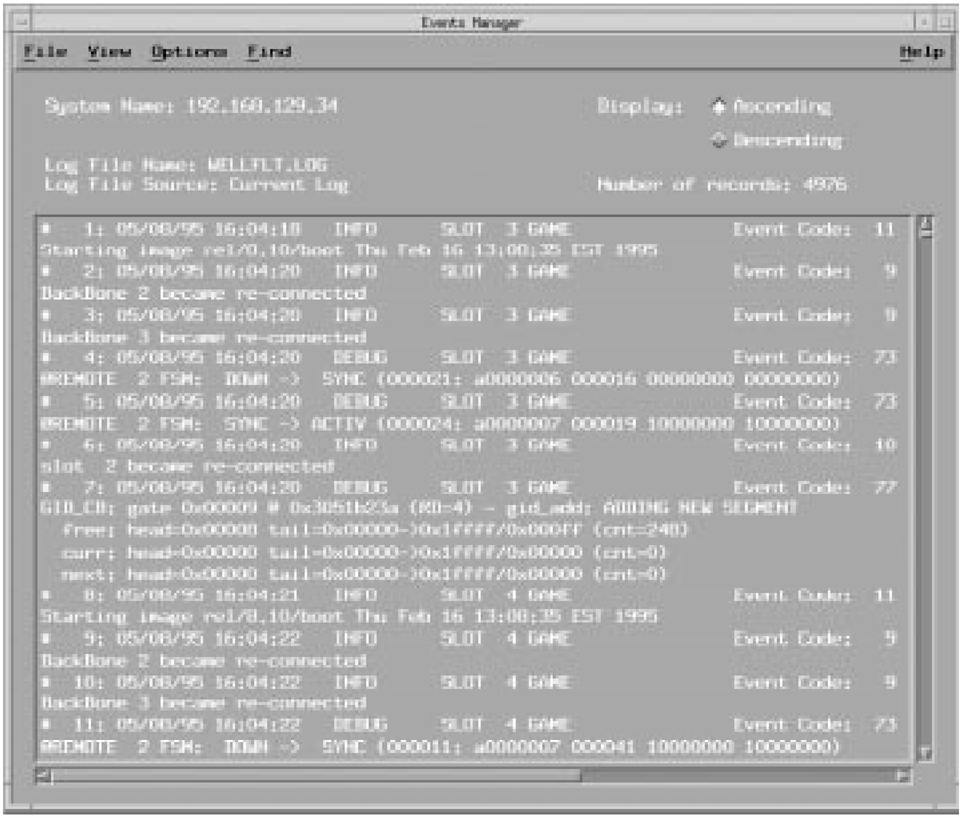
In the Trap Monitor window, choose File > Clear History File.

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

Monitoring Router Events

To monitor router events, you use the Events Manager. You access the Events Manager from the main Site Manager window by choosing Tools > Events Manager or by clicking on the Events button.

Figure 7-15 shows an example of the Events Manager window with an event log displayed.



System Name: 192.168.129.34

Display: ● Ascending ○ Descending

Log File Name: WELLFLT.LOG
Log File Source: Current Log

Number of records: 4976

```
*   1: 05/08/95 16:04:18   INFO      SLOT  3 GAME                  Event Code:  11
Starting image rel/8.10/boot Thu Feb 16 13:08:35 EST 1995
*   2: 05/08/95 16:04:20   INFO      SLOT  3 GAME                  Event Code:   9
BackBone 2 became re-connected
*   3: 05/08/95 16:04:20   INFO      SLOT  3 GAME                  Event Code:   9
BackBone 3 became re-connected
*   4: 05/08/95 16:04:20   DEBUG     SLOT  3 GAME                  Event Code:  73
#REMOTE  2 FSM:  DOWN ->  SYNC (000021: a0000006 000016 00000000 00000000)
*   5: 05/08/95 16:04:20   DEBUG     SLOT  3 GAME                  Event Code:  73
#REMOTE  2 FSM:  SYNC -> ACTIV (000024: a0000007 000019 10000000 10000000)
*   6: 05/08/95 16:04:20   INFO      SLOT  3 GAME                  Event Code:  10
slot  2 became re-connected
*   7: 05/08/95 16:04:20   DEBUG     SLOT  3 GAME                  Event Code:  77
GID_CB: gate 0x00009 # 0x3051b23a (RD=4) - gid_add: ADDING NEW SEGMENT
  free: head=0x00000 tail=0x00000->0x1ffff/0x000ff (cnt=240)
  curr: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
  next: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
*   8: 05/08/95 16:04:21   INFO      SLOT  4 GAME                  Event Code:  11
Starting image rel/8.10/boot Thu Feb 16 13:08:35 EST 1995
*   9: 05/08/95 16:04:22   INFO      SLOT  4 GAME                  Event Code:   9
BackBone 2 became re-connected
*  10: 05/08/95 16:04:22   INFO      SLOT  4 GAME                  Event Code:   9
BackBone 3 became re-connected
*  11: 05/08/95 16:04:22   DEBUG     SLOT  4 GAME                  Event Code:  73
#REMOTE  2 FSM:  DOWN ->  SYNC (000011: a0000007 000041 10000000 10000000)
```

Figure 7-15. Events Manager Window

The Events Manager menu bar includes the following options:

File -- Lets you retrieve and load log files, save the output to disk, and exit the Events Manager.

View -- Lets you refresh the display, clear the Events Manager window, and access filter options.

Options -- Lets you connect to the router.

Find -- Lets you search for messages that contain specific text.

For suggested responses to specific event messages, refer to *Event Messages for Routers*.

Use the Events Manager to do the following:

- Display event logs.
- Filter event messages.
- Search for an event message in the events log.
- Reload an event log saved in binary format back into the Events Manager window.

  (Storing a log on a router diskette or memory card saves the log in binary format.)
- Refresh the Events Manager window.
- Clear the Events Manager window.
- Save event messages to an ASCII file on your workstation. You can then view or print the file.
- Clear the current event log.

In addition to the Events Manager, on UNIX workstations you can use the UNIX *syslog* facility to gather information about the router. Using the syslog facility, you can specify a destination to which the router can forward event messages. For example, you can specify a file on a remote host to receive event messages. You can then open or print the event messages file.

For information about using the syslog facility, refer to Appendix D, “Configuring the syslog Facility.”

Viewing Event Messages

You view events messages for one router at a time. The router's event messages are collected in an *event log*. To view the router's event log, you can use the Events Manager, which retrieves the log from the router to which you are connected.

The Events Manager does not display event messages in real time.

You can scroll through the event messages using the window scroll bars (refer to Figure 7-15). Choose Ascending to display events from the oldest to the most recent. Choose Descending to display events from the newest (most recent) to the oldest.

Table 7-5 describes the contents of the event log displayed by the Events Manager.

Table 7-5. Event Message Details

Column	**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 the event message
Slot	Slot hosting the entity that generated the event message
Entity	Abbreviated name of the entity that generated the event message. Refer to *Event Messages for Routers* for information about each event code.
Event code	Event code. Refer to *Event Messages for Routers* for information about each event code.
Description	Text describing the event

Loading the Event Log into the Events Manager

You must load an event log into the Events Manager window to view event messages. There are three types of event logs:

- The *current log* in the router's active memory
- The *remote log* on the router's flash memory
- The *local log* stored locally (in binary format) on the Site Manager workstation

You must transfer and save the log on the Site Manager workstation using the Router Files Manager TFTP option. Refer to Chapter 5 for instructions. For each log file that you retrieve, you see the following information at the top of the Events Manager window (refer to Figure 7-15):

- The Log File Name field listing the name of the log file
- The Log File Source field with `Current Log, Remote Log, or Local Log`
- The Number of records field listing the total number of events

Loading the Current Log

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

To display the event messages in a router's current log:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Events Manager, unless you connected to the router from the Events Manager.**

   The Events Manager window opens (refer to Figure 7-15).

3. **Choose File > Get Current Log File.**

   The event messages in the current log now appear in the Events Manager window (refer to Figure 7-15).

4. **Choose File > Exit when you are done viewing the log file.**

   You return to the main Site Manager window.

Loading the Remote Log

A remote log resides in the router's flash memory.

To display the log:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Events Manager, unless you connected to the router from the Events Manager.**

   The Events Manager window opens (refer to Figure 7-15).

3. **Choose File > Get Remote Log File.**

   The Load Remote Log File window opens (Figure 7-16).

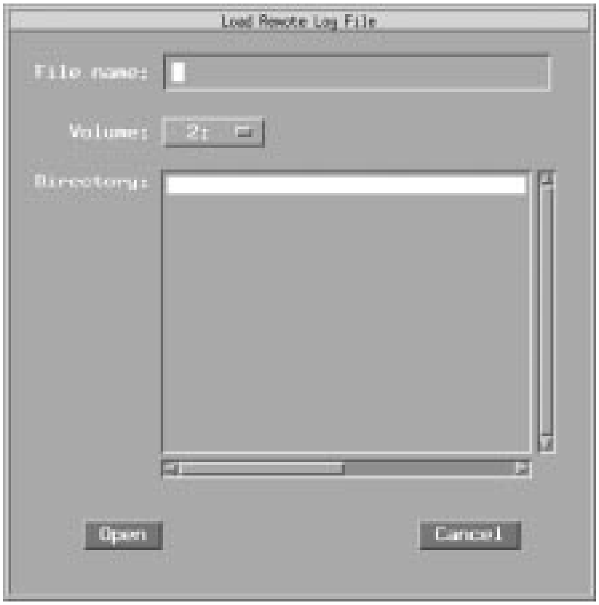


Figure 7-16. Load Remote Log File Window

4. **Type the file name of the event log in the format** *<filename>.log***.**

   Use the Router Files Manager to display a list of files on the router (refer to Chapter 5).

5. **Select the volume that contains the log file in the Volume field.**

6. **Click on Open.**

   The router transfers the file and displays it in the Events Manager window.

7. **Choose File > Exit when you are done viewing the log file.**

   You return to the main Site Manager window.

Loading a Local Log

A local log resides on the hard drive of your Site Manager workstation.

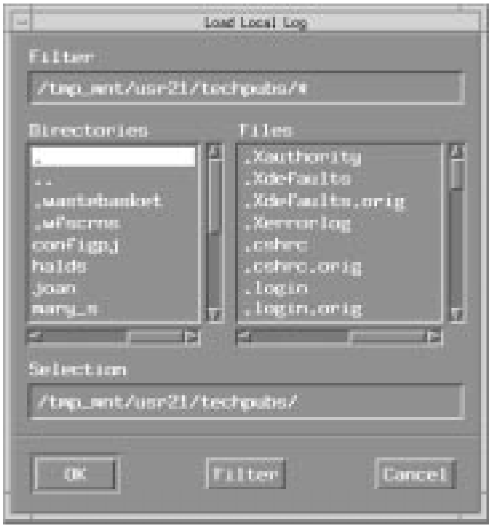
To display the local log:

1. **In the main Site Manager window, choose Tools > Events Manager.**

   The Events Manager window opens (refer to Figure 7-15).

2. **Choose File > Load Local Log File.**

   The Load Local Log window opens (Figure 7-17).



Filter: /tmp_mnt/usr21/techpubs/*

Directories:

```
.
..
.wastebasket
.wfscrns
configpj
halds
joan
mary_s
```

Files:

```
.Xauthority
.Xdefaults
.Xdefaults.orig
.Xerrorlog
.cshrc
.cshrc.orig
.login
.login.orig
```

Selection: /tmp_mnt/usr21/techpubs/

Figure 7-17. Load Local Log Window

3. **Select the directory from the Directories list and the log file from the Files list.**

The path appears in the Selection field.

4. **Click on OK.**

   The router displays the file residing on the workstation in the Events Manager window.

5. **Choose File > Exit when you are done viewing the log file.**

   You return to the main Site Manager window.

Filtering Event Messages

You can select the types of event messages to display in the Events Manager window by specifying filters. You can filter event messages by event severity, router slot, and protocol entity.

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 the source file.

To filter event messages:

1. **Load the event log into the Events Manager window.**

   Refer to "Loading the Event Log into the Events Manager" on page 7-26.

   The Events Manager window opens (refer to Figure 7-15).

2. **In the Events Manager window, choose View > Filters.**

   The Filtering Parameters window opens (Figure 7-18).

   In this window the options (parameters) that determine the messages you will see are highlighted. Click on Toggle to make a highlighted option unhighlighted, and the reverse.

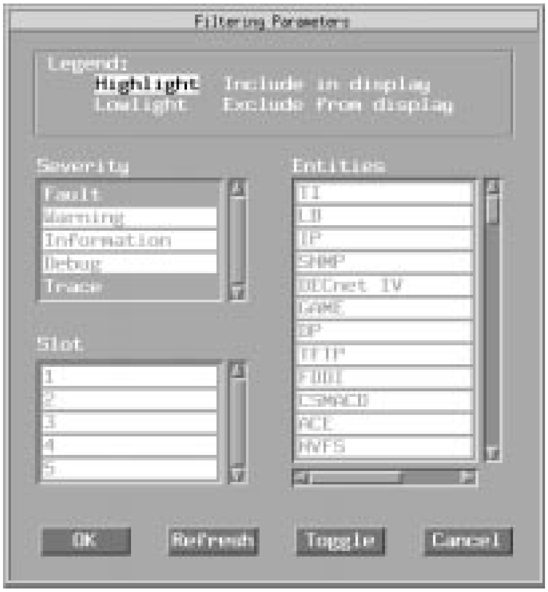


Figure 7-18. Filtering Parameters Window

3. **Select or deselect any Severity, Slot, or Entities option to modify the event log display.**

4. **Click on Refresh to view the event messages with the new filter.**

5. **Click on OK to save your changes.**

   You return to the Events Manager window.

   When you save you save only the changes. Only the Refresh option filters the event messages to reflect the changes you made.

   When you filter messages, the number of records does not change; the total number of event messages is always displayed.

Searching for an Event Message

You can use the Find and Find Next options in the Events Manager window to locate an event message containing specific text. This can make troubleshooting more efficient.

To locate a specific event message:

1. **Load the event log into the Events Manager window.**

   Refer to "Loading the Event Log into the Events Manager" on page 7-26.

2. **In the Events Manager window, choose Find > Find.**

   The Find Text Pattern window opens (Figure 7-19).

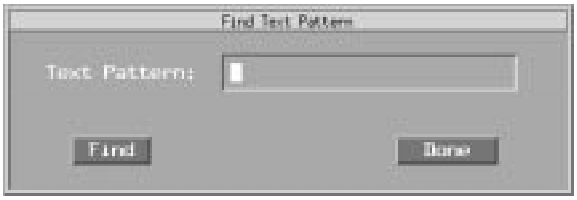


Figure 7-19. Find Text Pattern Window

3. **Type the text you want to find.**

   You can enter up to 255 characters (including spaces) in this field.

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

4. **Click on Find.**

   The Events Manager searches the event log until it finds the first instance of the text pattern. It then highlights that event message.

5. **Choose Find > Find Next to find the next instance of the same text pattern.**

6. **Click on Done to close the Find Text Pattern window.**

   You return to the Events Manager window.

Refreshing the Events Manager Window

To refresh the display in the Events Manager window, for example, after you filter event messages, choose View > Refresh Display.

Clearing the Events Manager Window

To clear the event messages in the Events Manager window, choose View > Clear Window. The window remains empty until you load an event log or refresh the display.

Saving Event Messages

You can save the event messages in the Events Manager window to an ASCII file on your Site Manager workstation. You can then print the log.

To save an event log to an ASCII file:

1. **Load the event log into the Events Manager window.**

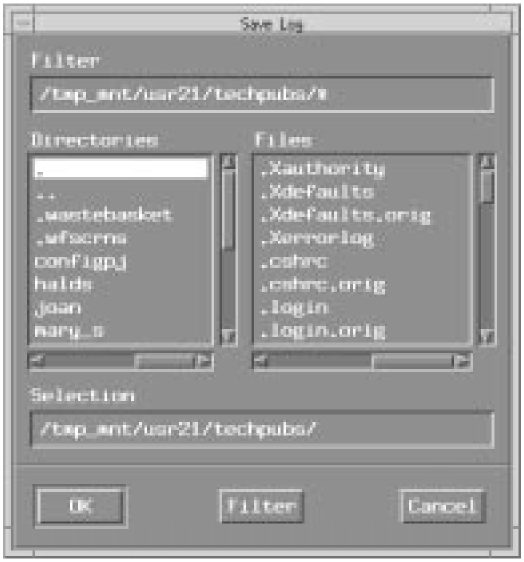
   Refer to "Loading the Event Log into the Events Manager" on page 7-26.

2. **If you want, filter the event messages displayed.**

   Refer to "Filtering Event Messages" on page 7-30.

3. **Choose File > Save Output to Disk.**

   The Save Log window opens (Figure 7-20).



Filter
/tmp_mnt/usr21/techpubs/*

Selection
/tmp_mnt/usr21/techpubs/

Figure 7-20. Save Log Window

4. **Select the path and file name from the Directories and Files lists to specify where you want to save the file.**

   The path appears in the Selection field.

5. **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.)

   For viewing purposes, you can reload event logs saved in binary format into the Events Manager, but you cannot reload event logs saved in ASCII format.

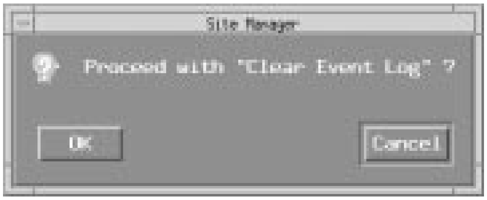
Clearing the Current Event Log

The router’s event log can hold only a fixed number of messages. When the file reaches its limit, the Events Manager starts overwriting the log from the beginning.

To clear a router’s current event log:

1. **In the main Site Manager window, choose Administration > Clear Event Log.**

   A confirmation window opens (Figure 7-21).



Proceed with "Clear Event Log" ?

Figure 7-21. Confirmation Window for Clearing Event Log

2. **Click on OK.**

   This deletes 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.

Chapter 8
Monitoring Statistics

The Statistics Manager enables you to gather statistical information that tells you how a router is operating in the network. Specifically, the Statistics Manager uses an SNMP-based polling mechanism to request the following:

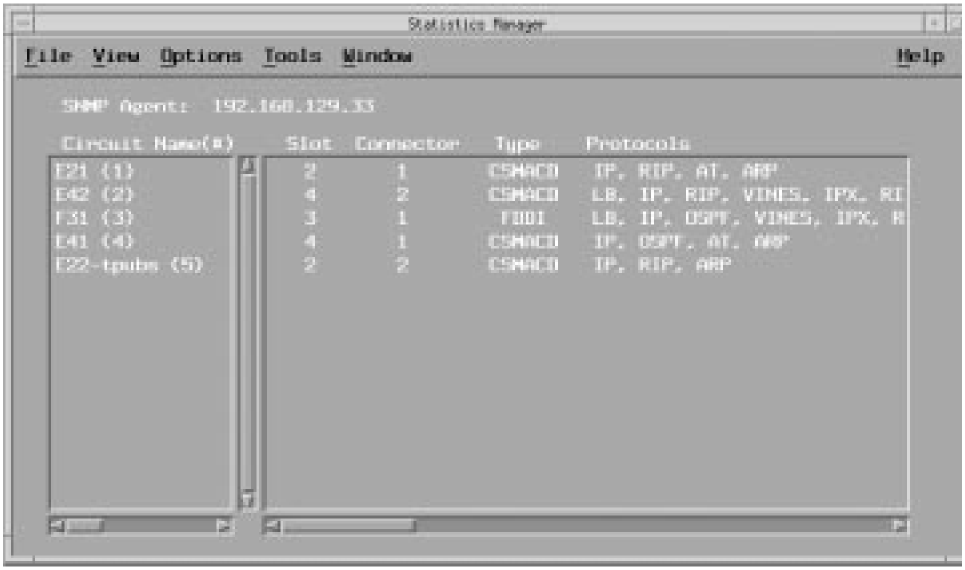
- Real-time data link layer statistics providing circuit information
- Network layer statistics providing protocol information

Site Manager displays the information in a statistics window. This chapter explains how to use the Statistics Manager to view statistics information.

The chapter contains the following information:

Statistics Manager Tool

To access the Statistics Manager, begin at the main Site Manager window and click on the Statistics function button or choose Tools > Statistics Manager. The Statistics Manager window opens (Figure 8-1).



SNMP Agent: 192.168.129.33

Circuit Name(#)	Slot	Connector	Type	Protocols
E21 (1)	2	1	CSMACD	IP, RIP, AT, ARP
E42 (2)	4	2	CSMACD	LB, IP, RIP, VINES, IPX, RI
F31 (3)	3	1	FDDI	LB, IP, OSPF, VINES, IPX, R
E41 (4)	4	1	CSMACD	IP, OSPF, AT, ARP
E22-tpubs (5)	2	2	CSMACD	IP, RIP, ARP

Figure 8-1. Statistics Manager Window

The menu bar in the Statistics Manager window contains the following options:

File -- Lets you exit the tool.

View -- Lets you refresh the display.

Options -- Lets you connect to the router.

Tools -- Lets you access Statistics Manager tools.

Window -- Lets you display a particular window.

Depending on whether you operate Site Manager on a UNIX workstation or a PC, the Statistics Manager stores all statistics window files in one of the following directories (Table 8-1).

Table 8-1. Location of Statistics Window Files

Platform	Default Window Directory	Custom Window Directory
UNIX workstation	*/usr/wf/lib/.wfscrns*	*$(HOME)/.wfscrns*
PC	*\wf\lib\wfscrns*	*\wf\wfscrns*

Statistics Manager Tools

The Statistics Manager provides four tools that you can access from the Statistics Manager's Tools menu (Figure 8-2).

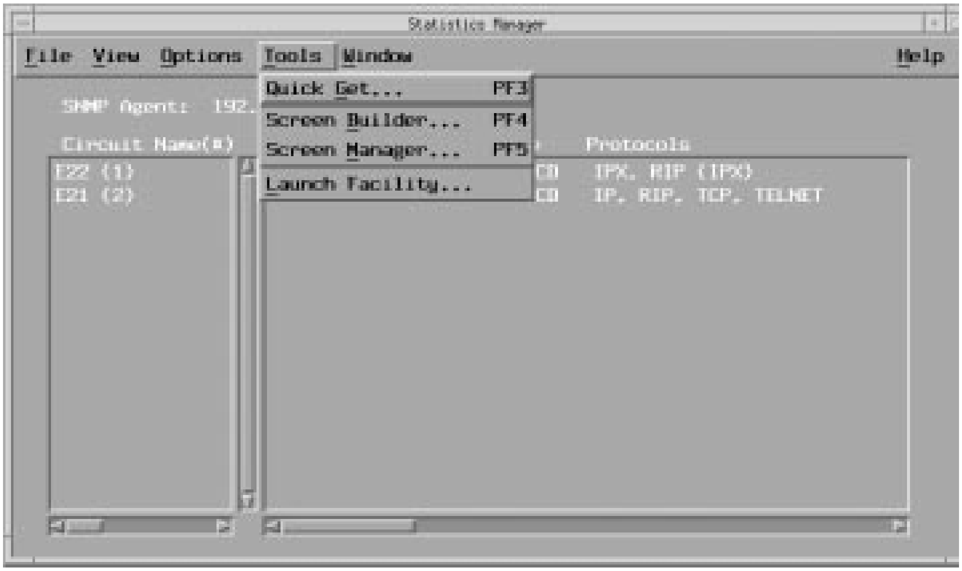


Figure 8-2. Statistics Manager Tools Menu

Table 8-2 lists each Statistics Manager tool.

Table 8-2. Statistics Manager Tools

Tool	Use to
Quick Get	View objects in the Bay Networks MIB.
Screen Builder	Design custom statistics windows.
Screen Manager	Manage your statistics window database and specify a current statistics window list.
Launch Facility	Select and display statistics windows from a current list of windows.

The following sections describe each of these tools.

Quick Get Tool

The Quick Get tool lets you view the MIB and retrieve instances of selected MIB objects from the router. The Bay Networks MIB is a Bay Networks proprietary database that contains the router's configuration parameters and statistics.

Quick Get enables you to debug your network, for example, by monitoring MIB objects, and provides an easy way to view the MIB and decide which objects you want to include in your customized statistics windows.

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

Screen Builder Tool

The Screen Builder tool lets you create custom statistics screens. The MIB browser lets you select up to nine objects to be included in a window. For each object you select, you design the display of the statistics window as follows:

- Column heading
- Column width
- Format of the display (decimal or hexadecimal)

You can also use the Screen Builder to edit custom windows. For example, you can redefine the display, and add or delete objects from the window.

Screen Manager Tool

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

Launch Facility Tool

The Launch Facility tool lets you retrieve and display any statistics windows that are in the current screen list. When you retrieve statistics from the router, the Statistics Manager polls the router for all instances of the MIB objects that you specified in the window, then it formats and displays the data in columns.

There are two modes in which the Statistics Manager retrieves statistics:

- *Circuit mode* -- The Statistics Manager continually polls the router for statistics and updates the statistics window with new data. You can specify how often the Statistics Manager polls the routers for statistics.
- *Table mode* -- The Statistics Manager retrieves statistics from the router only once -- when you display the window. You must refresh the window each time you want to update it with new data.

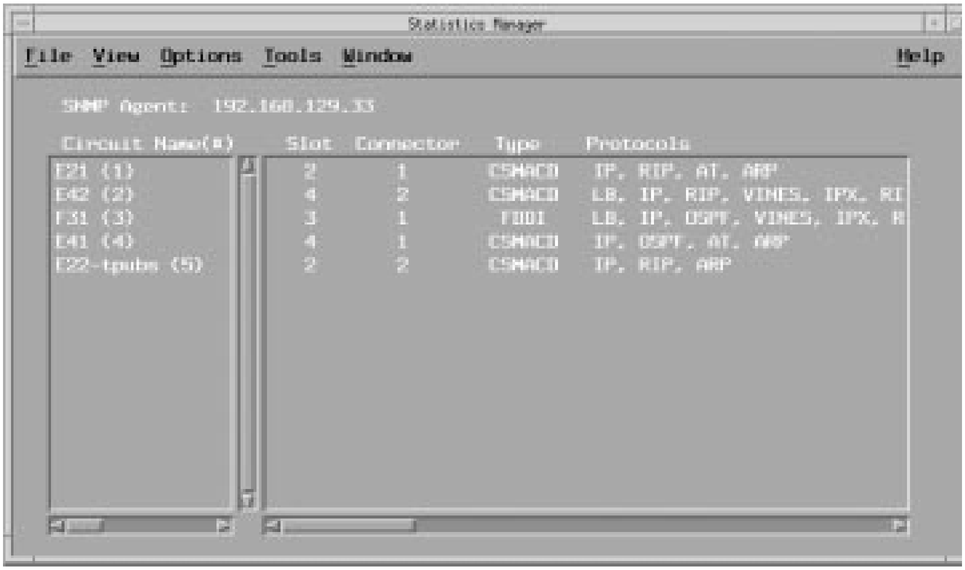
Circuit mode is predetermined for the default statistics windows. If you build custom statistics windows, you can specify the mode in which statistics are retrieved.

Using Online Help

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

Accessing Statistics

You access all router statistics from the Statistics Manager window. To access this window, begin at the main Site Manager window and click on Statistics, or choose Tools > Statistics Manager. The Statistics Manager window opens (Figure 8-3).



SNMP Agent: 192.168.129.33

Circuit Name(#)	Slot	Connector	Type	Protocols
E21 (1)	2	1	CSMACD	IP, RIP, AT, ARP
E42 (2)	4	2	CSMACD	LB, IP, RIP, VINES, IPX, RI
F31 (3)	3	1	FDDI	LB, IP, OSPF, VINES, IPX, R
E41 (4)	4	1	CSMACD	IP, OSPF, AT, ARP
E22-tpubs (5)	2	2	CSMACD	IP, RIP, ARP

Figure 8-3. Statistics Manager Window

The Statistics Manager requires an active connection to a router to display router statistics. You can connect to a router before accessing the Statistics Manager or from within the Statistics Manager using Options from the menu bar. Refer to Chapter 1 for instructions.

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.

From the Statistics Manager window, you perform any statistics task.

Defining the Current Screen List

The current screen list is a subset of the default statistics windows and any custom statistics windows you built to display statistics. (Refer to "Building Custom Statistics Windows" on page 8-22 for information about designing custom statistics windows.)

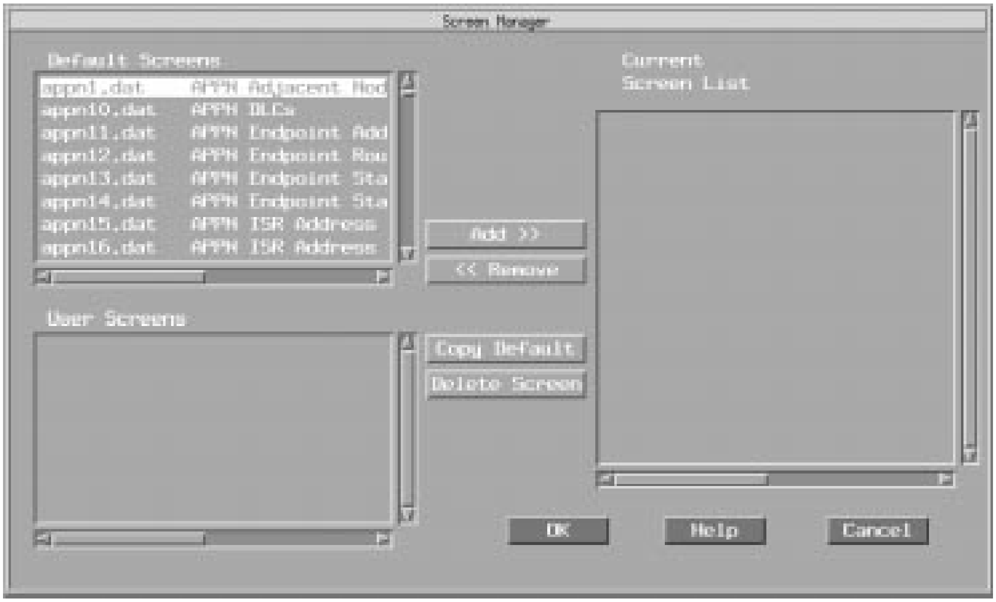
When you first start the Statistics Manager, there are no available statistics windows. To view statistics, you must add statistics windows to the current screen list. Add only those statistics windows that you use most often. This will help you to manage your statistics window database most effectively.

Adding Statistics Windows

To add a statistics window to the current screen list:

1. **In the Statistics Manager window, choose Tools > Screen Manager.**

   The Screen Manager window opens (Figure 8-4).



```
appn1.dat      APPN Adjacent Nod
appn10.dat     APPN DLCs
appn11.dat     APPN Endpoint Add
appn12.dat     APPN Endpoint Rou
appn13.dat     APPN Endpoint Sta
appn14.dat     APPN Endpoint Sta
appn15.dat     APPN ISR Address
appn16.dat     APPN ISR Address
```

Figure 8-4. Screen Manager Window

In the Default Screens list, the Screen Manager displays the default statistics windows, grouped by protocol. Use the scroll bar to view the list.

The Statistics Manager identifies each default statistics window using a file name with the *.dat* extension, followed by a description of the data the window displays. Figure 8-5 shows the IP routing statistics window title.

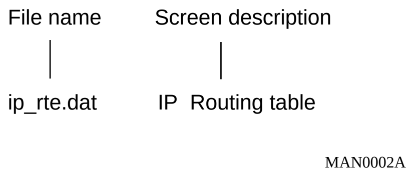


Figure 8-5. Example of File Name and Window Description

The User Screens list, below the Default Screens list, is empty if you have not yet built any custom statistics windows using the Screen Builder.

2. **From the Default Screens list, select a statistics window that you want to add to the Current Screen List.**
3. **Click on Add.**

   The Current Screen List can contain both default windows and custom windows.

4. **Repeat steps 2 and 3 to add more windows to the current screen list.**
5. **Click on OK to update the current screen list and save your changes.**

   The Statistics Manager updates the Current Screen List to include the statistics windows that you add.

   Click on Cancel to exit the Screen Manager window without saving.

6. **Go to one of the following sections:**
   - To remove statistics windows from the current screen list, go to "Removing Statistics Windows" on page 8-9.
   - To retrieve statistics from the router and display them, go to "Retrieving Statistics" on page 8-10.

Removing Statistics Windows

To remove a statistics window from the Current Screen List:

1. **In the Statistics Manager window, choose Tools > Screen Manager.**

   The Screen Manager window opens (refer to Figure 8-4).

2. **Select the statistics window you want to remove from the current screen list.**

3. **Click on Remove.**

   The Statistics Manager removes the statistics screen you selected.

4. **Repeat steps 2 and 3 to remove additional statistics windows from the current screen list.**

5. **Click on OK to exit the window and save your changes.**

   Click on Cancel to exit without saving the changes.

6. **Go to "Retrieving Statistics" on page 8-10 to retrieve statistics from the router and display them.**

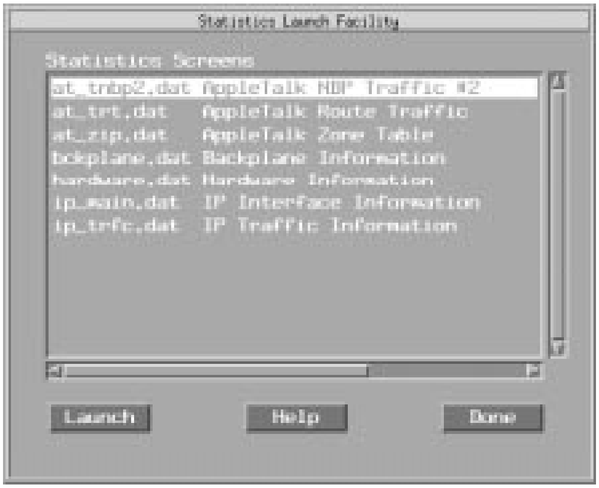
Retrieving Statistics

Use the Launch Facility to retrieve statistics from the router and display them in a window. Before you can display a statistics window, you must add it to the current screen list. For instructions, refer to “Defining the Current Screen List” on page 8-7.

To retrieve statistics from the router:

1. **In the Statistics Manager window, choose Tools > Launch Facility.**

   The Statistics Launch Facility window opens, displaying the statistics windows from the current screen list (Figure 8-6).



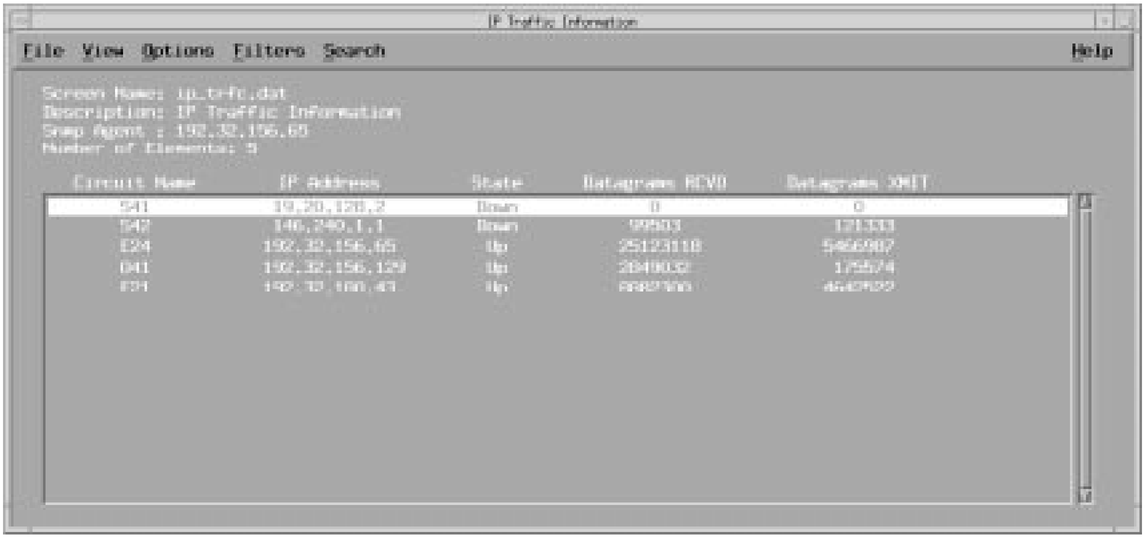
at_trbp2.dat	AppleTalk NBP Traffic #2
at_trt.dat	AppleTalk Route Traffic
at_zip.dat	AppleTalk Zone Table
bckplane.dat	Backplane Information
hardware.dat	Hardware Information
ip_main.dat	IP Interface Information
ip_trfc.dat	IP Traffic Information

Figure 8-6. Statistics Launch Facility Window

2. **Select one of the statistics windows.**

3. **Click on Launch.**

   Site Manager retrieves the specified MIB objects from the router and opens a window, which displays the statistics. For example, Figure 8-7 shows the IP Traffic Information statistics window.



```
Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5

   Circuit Name        IP Address        State     Datagrams RCVD     Datagrams XMIT
       S41           19.20.128.2         Down            0                  0
       S42           146.240.1.1         Down          99503             121333
       E24          192.32.156.65         Up         25123118            5466987
       D41          192.32.156.129        Up          2849032             175574
       E21          192.32.188.43         Up          8882700            4642522
```

Figure 8-7. Retrieved Statistics Display

Refreshing Active Statistics Windows

To update a statistics window, choose View > Refresh Display.

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

Stopping Statistics Retrieval

To stop the Statistics Manager from collecting any further statistics, choose View > Stop Retrieval.

You can then choose File > Exit to exit the Statistics Manager.

Specifying the Circuit Mode Polling Rate

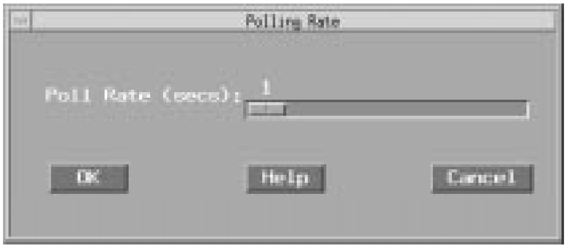
When the Statistics Manager retrieves statistics in circuit mode, it continually polls the router for statistics and updates the statistics windows with new data. If you watch the window, the information will keep changing.

The Statistics Manager retrieves statistics in circuit mode for default statistics windows. However, you can specify the number of seconds that the Statistics Manager waits between polls to the router.

To specify the polling rate:

1. **In any statistics window, choose Options > Poll Rate.**

   The Polling Rate window opens (Figure 8-8).



Poll Rate (secs): 1

Figure 8-8. Polling Rate Window

2. **Use the slide bar to specify a polling rate, then click on OK.**

   You return to the previous statistics window.

Zeroing Circuit Mode Statistics

You can reset all counters in a circuit mode statistics window to 0 using the Zero All Counters option. You can also reset the counters in a selected row to 0 using the Zero Current Row Counters option.

When you reset a counter to 0, the Statistics Manager stores the value of the counter at that moment and uses this value as a reference point. When the counter display resumes, the Statistics Manager displays the difference between the counter's current value and the last known reference value.

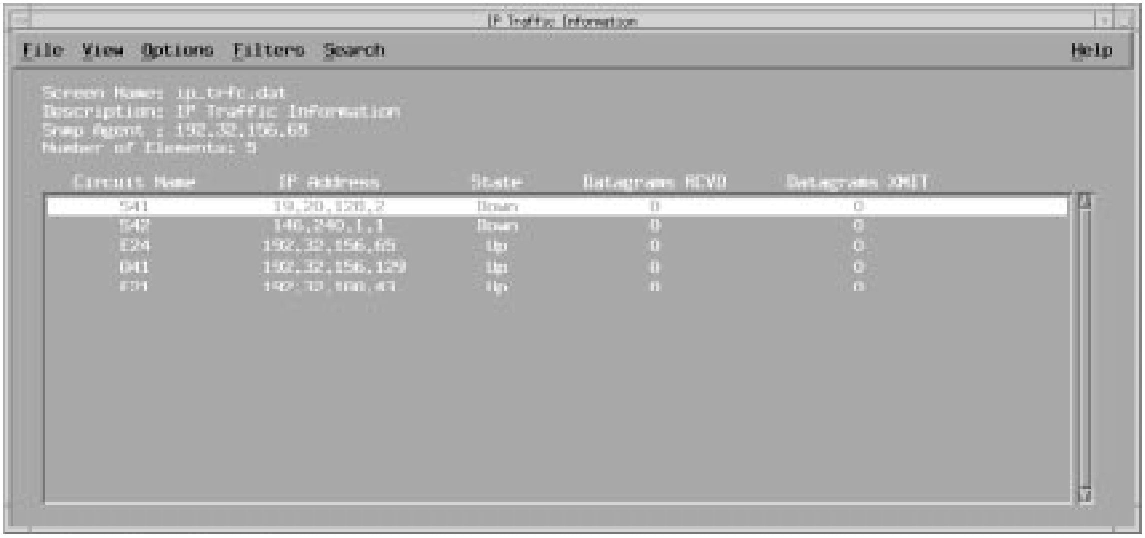
Zeroing a counter affects only the values displayed by the Statistics Manager and has no effect on the actual value of counter objects in the router's MIB. If you close the Statistics Manager, then restart it, you will see the actual value of the counter in the MIB, not the value displayed after resetting the counter.

The next sections explain how to zero the counters in a circuit mode window.

Zeroing All Counters in a Window

To clear all counters, choose Options > Zero All Counters.

Figure 8-9 shows a typical response to the Zero All Counters option.



Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5

Circuit Name	IP Address	State	Datagrams RCVD	Datagrams XMIT
S41	19.20.128.2	Down	0	0
S42	146.240.1.1	Down	0	0
E24	192.32.156.65	Up	0	0
O41	192.32.156.129	Up	0	0
E21	192.32.180.43	Up	0	0

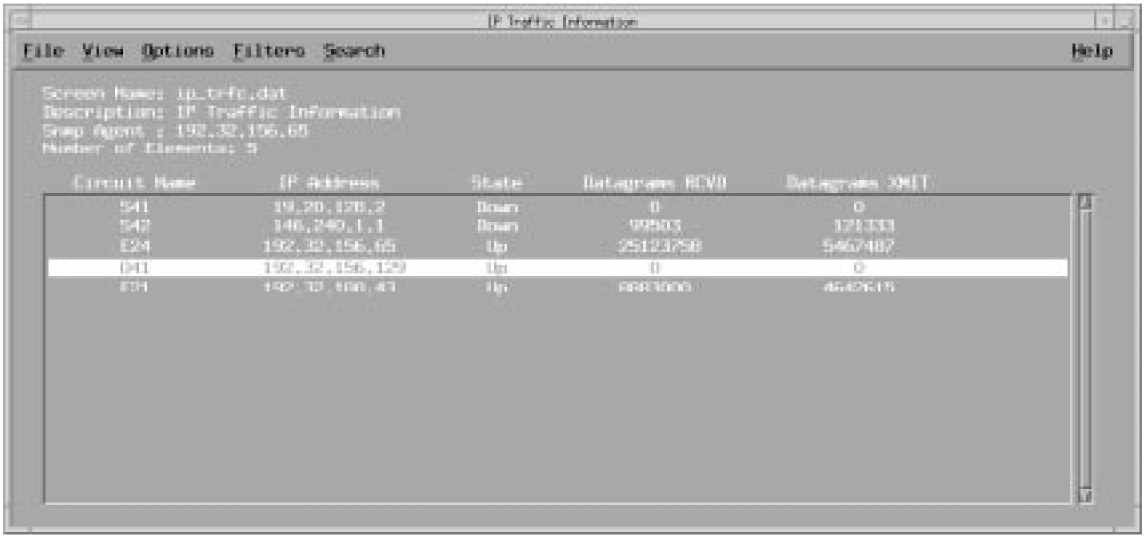
Figure 8-9. Zeroing All Counters in a Window

In this example, the counters Datagrams RCVD and Datagrams XMIT are reset to 0. This type of reset has no effect on the current values of these counter objects in the MIB.

Zeroing All Counters in a Specific Row

To clear all counters in a specific row, select a row, then choose Options > Zero Current Row Counters.

Figure 8-10 shows a typical response to the Zero Current Row Counters option.



Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5

Circuit Name	IP Address	State	Datagrams RCVD	Datagrams XMIT
S41	19.20.128.2	Down	0	0
S42	146.240.1.1	Down	99503	121333
E24	192.32.156.65	Up	25123758	5467487
D41	192.32.156.129	Up	0	0
E21	192.32.168.43	Up	8883000	4642615

Figure 8-10. Zeroing All Counters in a Specific Row

The counters Datagrams RCVD and Datagrams XMIT are reset to 0 in the selected row. The reset has no effect on the current values of these counter objects in the router MIB.

Creating Statistics Filters

Using the Launch Facility, you can set filters for each statistics window you open.

Normally, the Statistics Manager polls a router for the values of all MIB objects defined in the active statistics window. The window then shows the values of those objects, as determined by the data returned by the router. Filtering limits the objects you view in the statistics window.

There are two types of filters:

- Display filters
- Retrieval filters

A *display filter* enables the Statistics Manager to search the contents of the active statistics window and then show or hide the specified objects.

You can set the display filter to show or hide only those objects that contain a string matching the filter string. Specifying a longer display filter string narrows the number of possible matches in the active statistics window.

A *retrieval filter* enables the Statistics Manager to poll a router for only a subset of MIB objects. These objects have instance IDs that match the full or partial instance ID you enter in the Retrieval Filter window. Specifying a longer string for the instance ID in the Retrieval Filter window causes the workstation to solicit a smaller number of objects from a router.

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

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. It also reduces the amount of network bandwidth consumed by 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 the values of certain MIB objects, then apply a display filter to hide or show objects in the resulting statistics window.

Using Display Filters

To create a display filter:

1. **Open a statistics window using the Launch Facility.**
2. **Choose Filters > Display Filters.**

   The Display Filters window opens (Figure 8-11).

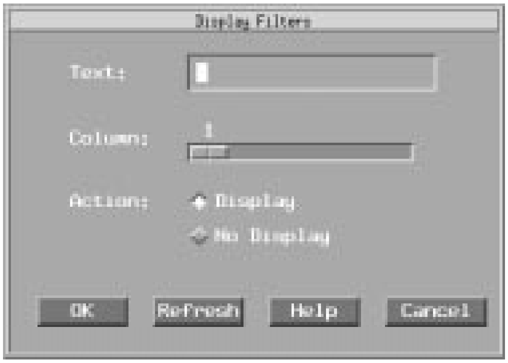


Figure 8-11. Display Filters Window

3. **Type the text string you want to use as the filter in the Text field.**
4. **Use the slide bar to select the column in the statistics window to which you want to apply the filter.**
5. **Determine whether you want to show or hide the filtered statistics.**
   - Choose Display to display only those statistics that match the filter.
   - Choose No Display to hide those statistics that match the filter.

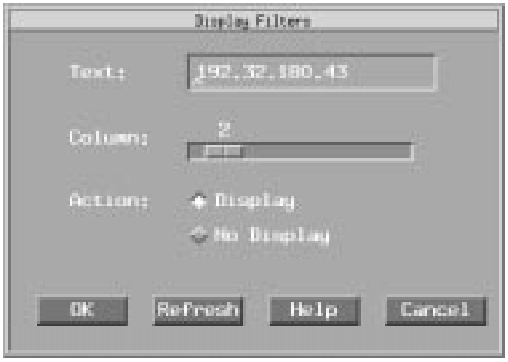
6. **Click on OK to save the filter in memory, or click on Refresh to implement the filter immediately.**

   - If you click on OK, the Display Filters window closes. There is no immediate change to the statistics window. However, the next time you refresh the statistics window, it displays only statistics specified by the filter.
   - If you click on Refresh, the Statistics Manager immediately refreshes the statistics window and displays only the statistics specified by the filter.

7. **Click on OK to exit the Display Filters window.**

Display Filter Example

To display only the statistics for a circuit with an IP address of 192.32.180.43, configure the display filter as shown in Figure 8-12.



Display Filters

Text: 192.32.180.43

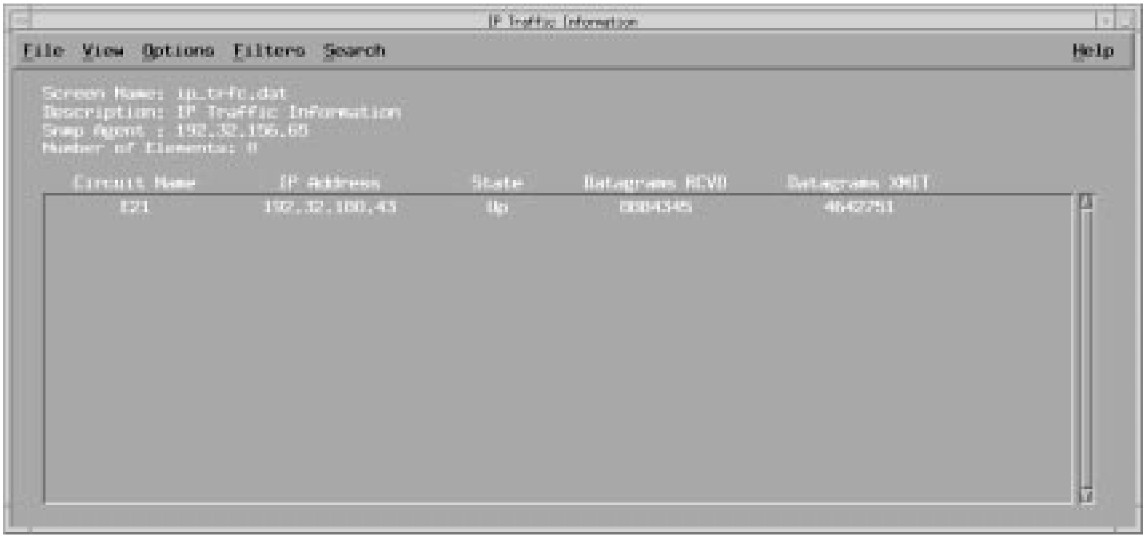
Column: 2

Action: ● Display
○ No Display

Figure 8-12. Sample Display Filters Window

When you click on Refresh in the Display Filters window, the Statistics Manager displays only the IP address 192.32.180.43 in column 2 of the active statistics window.

Figure 8-13 shows the result of applying the display filter.



```
Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.68
Number of Elements: 8

   Circuit Name        IP Address        State    Datagrams RCVD    Datagrams XMIT
       E21           192.32.180.43        Up         8884345           4642751
```

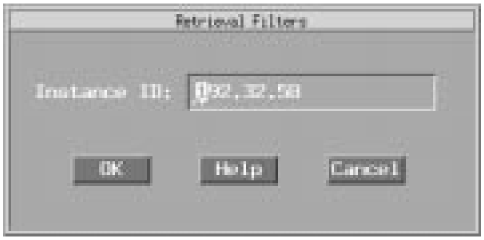
Figure 8-13. Statistics Window After Using a Display Filter

Using Retrieval Filters

To create a retrieval filter:

1. **Open a statistics window using the Launch Facility.**
2. **Choose Filters > Retrieval Filters.**

   The Retrieval Filters window opens (Figure 8-14).



Instance ID: 192.32.58

Figure 8-14. Retrieval Filters Window

3. **Type the instance ID of the object you want to view.**

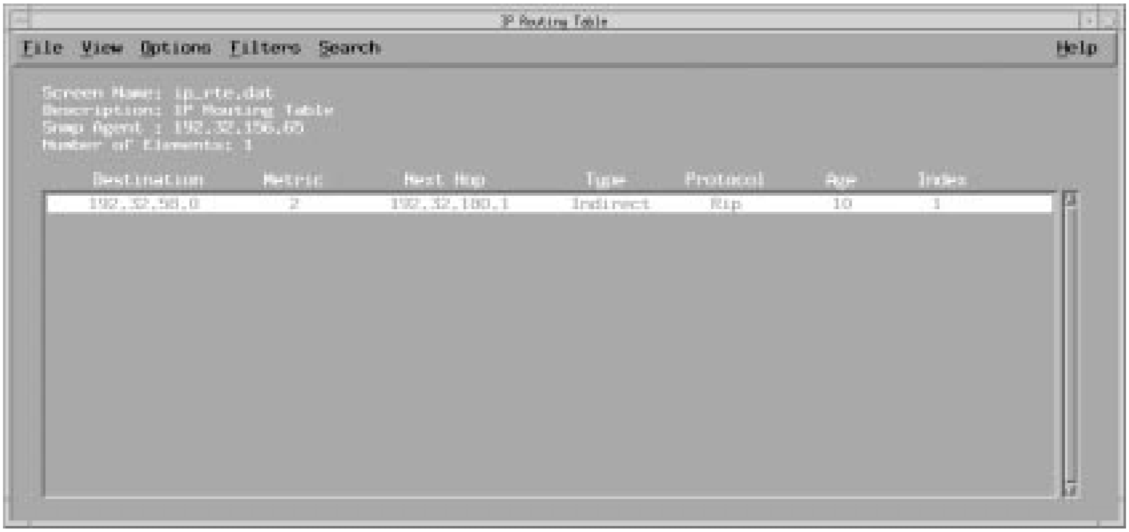
   Specifying a partial ID causes the Statistics Manager to poll and display all objects that begin with the same partial ID.

4. **Click on OK to save the filter in memory.**

   You return to the active statistics window.

5. **Choose View > Refresh Display.**

Figure 8-15 shows the result of this retrieval filter. In this case, 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.



Screen Name: ip_rte.dat
Description: IP Routing Table
Snmp Agent : 192.32.156.65
Number of Elements: 1

Destination	Metric	Next Hop	Type	Protocol	Age	Index
192.32.58.0	2	192.32.180.1	Indirect	Rip	10	1

Figure 8-15. Statistics Window After Using a Retrieval Filter

Searching for Information in a Statistics Window

You can search for any text string that appears in a statistics window.

To define the text string for the search:

1. **Open a statistics window using the Launch Facility.**
2. **In the active statistics window, choose Search > Find.**

   The Search Options window opens (Figure 8-16).

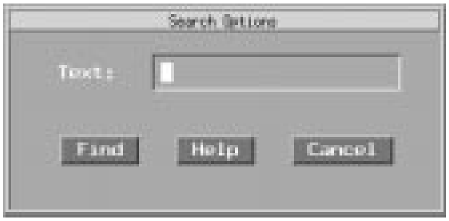


Figure 8-16. Search Options Window

3. **Enter the text you want to search for.**

   The Search Options window is case-sensitive.
4. **Click on Find.**

   The Statistics Manager selects the first line that includes the text string.
5. **Continue clicking on Find to search for other matching strings.**

   You can also search for other matching strings by clicking on Cancel in the Search Options window, then choosing Search > Find Next in the statistics window.

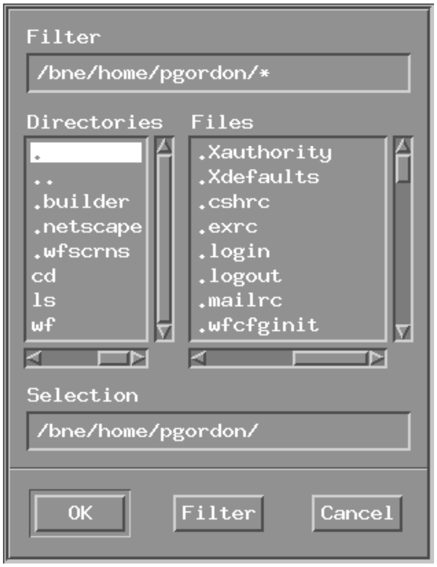
Saving Statistics Information in an ASCII File

The Statistics Manager lets you save the information displayed in a statistics window to an ASCII file on your Site Manager workstation.

To save the information shown in the statistics window:

1. **Choose File > Save As.**

   A window opens prompting you to choose a directory and file name for the statistics file (Figure 8-17).



Filter
/bne/home/pgordon/*

Directories
.
..
.builder
.netscape
.wfscrns
cd
ls
wf

Files
.Xauthority
.Xdefaults
.cshrc
.exrc
.login
.logout
.mailrc
.wfcfginit

Selection
/bne/home/pgordon/

Figure 8-17. Save As Window

2. **Select a directory for the file.**
3. **Type a file name.**
4. **Click on OK.**

   Site Manager saves the statistics in ASCII format to the named file.

   After you save the file, you can use any text editor to view the data.

Building Custom Statistics Windows

You can build custom statistics windows that include up to nine objects from the Bay Networks MIB and define the format of the statistics display. After you save the custom statistics window, it is added to the User Screens list in the Screen Manager window (refer to Figure 8-4).

Designing Custom Statistics Windows

To design a custom statistics window:

1. **In the Statistics Manager window, choose Tools > Screen Builder.**

   The Screen Builder Facility window opens (Figure 8-18).

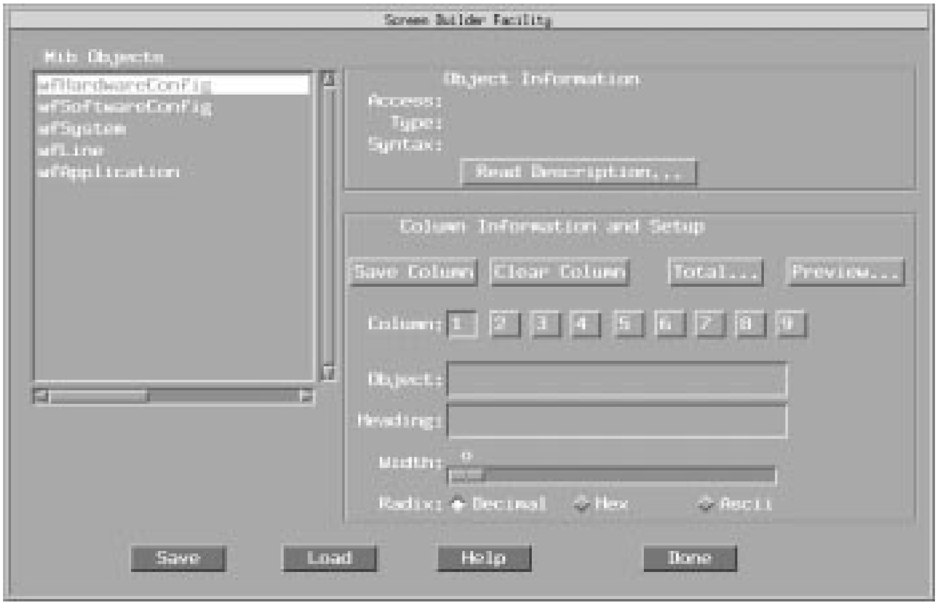


Figure 8-18. Screen Builder Facility Window

The MIB browser on the left side of the window lets you scroll through the MIB and select MIB objects to add to the statistics window. (Refer to “Using the MIB Browser” on page 8-32 to learn how to find objects in the MIB.) The Column Information and Setup portion of the window lets you specify how the statistics for the selected objects appear.

2. **Specify the column you want to define in the window by clicking on the corresponding column number.**

   For example, to define the first column in the statistics window, click on 1.

3. **Select the MIB object that you want listed in the column from the MIB Objects list.**

   The Object field displays the MIB object you select.

4. **In the Heading field, type a name that describes the type of statistics that will be displayed in the column selected in step 2.**

   For example, if you select the object wfIPInterfaceAddr, you could name the column *IP Address*.

5. **In the Width field, use the slide bar to select the column width.**

   The width is displayed in character units. The width you specify must be greater than 0 and greater than or equal to the column heading width. If any data exceeds the specified column width, the rest of the data on the same line moves 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. **In the Radix field, click on the appropriate button to specify whether the display uses decimal, hexadecimal, or ASCII format.**

   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.

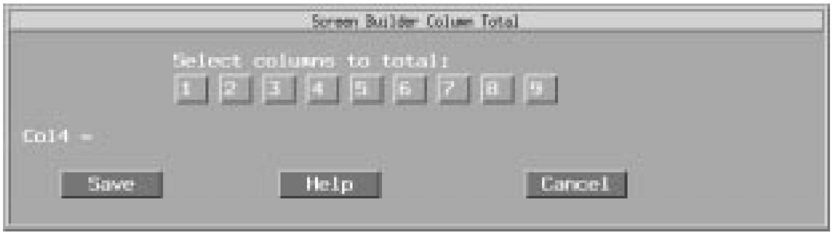
8. **Repeat steps 1 through 7 to add other columns to the statistics window.**

9. **To generate a sum of the values in two or more columns, follow these steps:**

   a. **Click on the number of the column that should display the sum.**

   b. **Click on Total.**

The Screen Builder Column Total window opens (Figure 8-19).



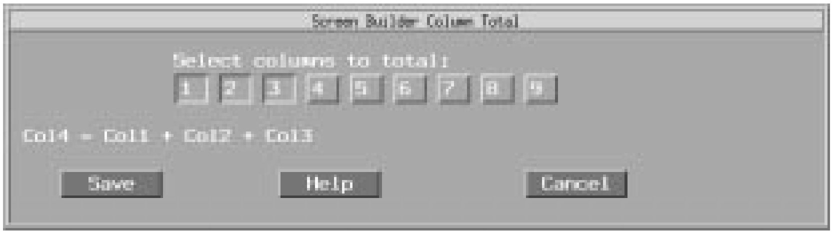
Col4 =

Figure 8-19. Screen Builder Column Total Window

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

For example, if 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 those three columns.

Figure 8-20 shows that column 4 will display the total of the values in columns 1, 2, and 3.



Col4 = Col1 + Col2 + Col3

Figure 8-20. Selecting Columns to Total

d. **Click on Save.**

You return to the Screen Builder Facility window.

e. **Click on Save Column to save the totals column you just specified.**

10. **Click on Preview to preview the statistics window you just built.**

The statistics window opens. Note, however, that the Statistics Manager does not retrieve any statistics from the router.

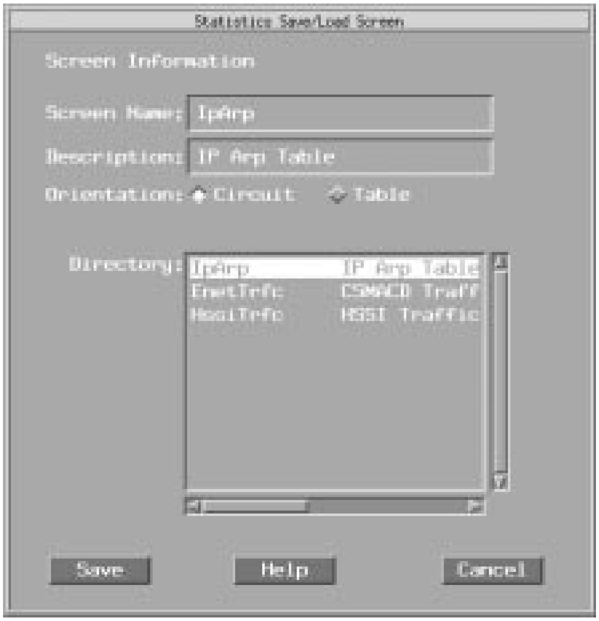
Saving the Custom Window to a File

After you design a custom statistics window, you can save it to a file for future use.

To save a custom statistics window:

1. **In the Screen Builder window, click on Save.**

   The Statistics Save/Load Screen window opens (Figure 8-21). It lists all the custom statistics window files that already exist in the directory.



Statistics Save/Load Screen

Screen Information

Screen Name: IpArp

Description: IP Arp Table

Orientation: ● Circuit ○ Table

Directory:

```
IpArp        IP Arp Table
EnetTrfc     CSMACD Traff
HssiTrfc     HSSI Traffic
```

Figure 8-21. Statistics Save/Load Screen Window

2. **Save the window to a new file according to the steps that follow, or go to step 3 to save the window to an existing file.**

   a. **In the Screen Name field, type a new name for the window.**

      If you are saving the file to a PC, the name you enter must follow standard file-naming conventions.

   b. **In the Description field, type a description of the window.**

      The maximum length of the window description is 40 characters.

   c. **Specify the mode by selecting either Circuit or Table.**

      Choose Circuit if you want the Statistics Manager to continually update the window with new statistics. Choose Table if you want the Statistics Manager to gather and display current statistics only once, when you retrieve statistics with the Launch Facility.

   d. **Click on Save to save the statistics window to a file.**

      Depending on whether you are running Site Manager on a UNIX workstation or PC, the Statistics Manager saves all custom statistics windows to the directory listed in Table 8-3:

Table 8-3. Directories for Custom Statistics Windows

Platform	Custom Window Directory
UNIX	$(HOME)/.wfscrns
PC	*\wf\wfscrns*

3. **To save the window to an existing file:**

   a. **Select the file from the list, then click on Save.**

   b. **The Statistics Manager confirms that you want to save the file. Click on OK to allow the Statistics Manager to overwrite the existing file.**

Using the Custom Statistics Window to Retrieve Statistics

To use the custom statistics window you created:

1. **Add the custom window to the current screen list.**

   See “Defining the Current Screen List” on page 8-7 for instructions.

2. **Use the Launch Facility to retrieve statistics in the custom window.**

   See “Retrieving Statistics” on page 8-10 for instructions.

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

Editing Statistics Windows

The default statistics windows are write-protected, so you cannot edit them. To customize a default window, copy it to the custom window directory on your Site Manager workstation under a new name. Then load and edit it as described in this section. You can also edit any custom window you created.

Loading a Statistics Window into the Screen Builder

Before you can edit a statistics window file, you must load it into the Screen Builder.

To load a statistics window file:

1. **In the Statistics Manager window, choose Tools > Screen Builder.**

   The Screen Builder Facility window opens (refer to Figure 8-18).

2. **Click on Load.**

   The Statistics Save/Load Screen opens (refer to Figure 8-21).

3. **Select the file you want to edit.**

   After you select a file, the Screen Information fields reflect the window name and type of data it collects.

4. **Click on Load to load the column attributes into the Screen Builder.**

   The Column Information and Setup portion of the Screen Builder Facility window now reflects the statistics window you loaded, beginning with the information for the first column.

Modifying the Statistics Window

After you load a statistics window into the Screen Builder, you can edit it.

To edit the window columns:

1. **Click on the number corresponding to the column you want to edit.**

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

2. **To remove all of the current column information, click on Clear Column.**
3. **Select and edit any of the column attributes, as follows:**

   - If you want the column to contain statistics about a different object, select a new object from the MIB Objects list.
   - To change the column size, use the slide bar 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.

   Refer to "Designing Custom Statistics Windows" on page 8-22 for information about setting each column attribute.

4. **Click on Save Column to implement your changes.**
5. **Repeat steps 3 and 4 to edit additional columns.**
6. **To see the results of your edits, click on Preview to view the window.**
7. **Click on Save to save your changes.**

   The Statistics Save/Load Screen opens (refer to Figure 8-21).

   You can save this modified window to an existing file or save it as a new file. Refer to "Saving the Custom Window to a File" on page 8-25 for instructions.

To view a new statistics window:

1. **Add the window to the current screen list.**

   See "Defining the Current Screen List" on page 8-7 for instructions.

2. **Use the Launch Facility to retrieve statistics in the custom window.**

   See "Retrieving Statistics" on page 8-10 for instructions.

Viewing the Bay Networks MIB

The Bay Networks MIB is a hierarchical database consisting of:

- Configuration and statistical objects that the router's Gate Access Management Entity (GAME) operating system uses
- Protocol image software that defines, limits, and monitors the behavior of a Bay Networks router in your network

The Bay Networks MIB includes all objects for every protocol that Bay Networks routers support. It is a specific extension of the Management Information Base II (MIB II) described in Internet Request for Comments (RFC) 1213.

Through Site Manager or the Technician Interface, you can:

- Read the values of many MIB objects with the **SNMP GET** command
- Write the values of a subset of MIB objects with the **SNMP SET** command

The GAME operating system also has exclusive read/write access to certain objects in the MIB. GAME uses the configuration file to create an active MIB that dictates the behavior of that router on your network.

Figure 8-22 shows the relationship between Site Manager and the Bay Networks MIB.

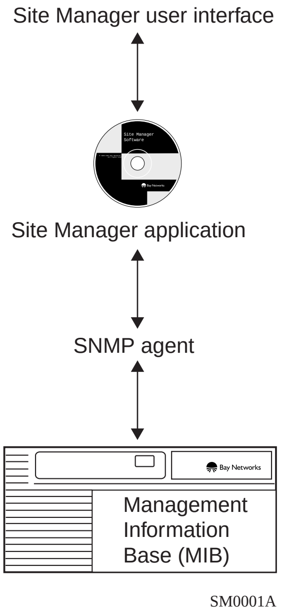


Figure 8-22. Accessing the Bay Networks MIB

Using Quick Get to View the MIB

To view the Bay Networks MIB, you use the Quick Get tool. To open the Quick Get tool, begin at the Statistics Manager window and choose Tools > Quick Get. The Quick Get Facility window opens (Figure 8-23).

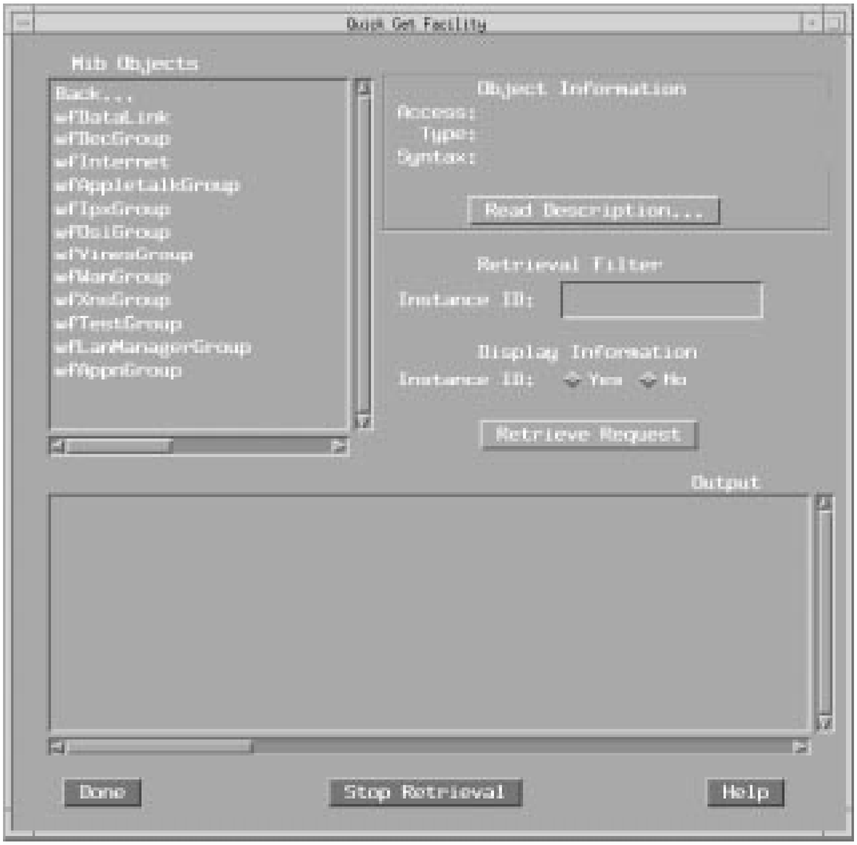


Figure 8-23. Quick Get Facility Window

Quick Get includes a MIB browser in the upper left corner that lets you scroll through the MIB Objects list and select up to 10 objects from the MIB. You then use Quick Get to retrieve all instances of the objects you select and to display that information in columns in the Quick Get Facility window.

Using the MIB Browser

The Bay Networks MIB is organized as a hierarchical tree. When you first activate Quick Get, it displays the top of the MIB tree. Navigate through the tree until you get to the Bay Networks MIB, called Wellfleet Series 7 MIB.

The list of object groups in the Bay Networks MIB is as follows:

- wfHardwareConfig
- wfSoftwareConfig
- wfSystem
- wfLine
- wfApplication
- rptrBasicPackage
- rptrMonitorPackage
- rptrAddrTrackPackage

Beneath these object groups, related objects are organized in subordinate object groups or tables. For example, Figure 8-24 shows part of the MIB tree for the wfSystem object group. The prefix *wf* that precedes many of the MIB objects indicates that they are Bay Networks enterprise-specific objects.

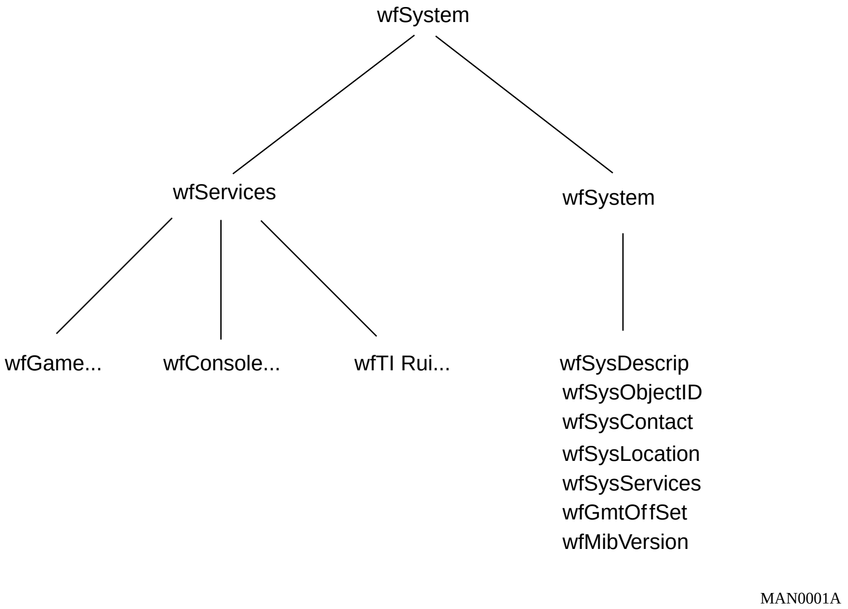


Figure 8-24. MIB Tree for System Object Group

To access individual objects, first select the top-level object group. The MIB browser displays subordinate object groups at the next level of the tree. 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 Objects list. To move backward in the MIB tree, select the Back option, which appears in the Quick Get Facility window after you display subordinate object groups from the top-level object group.

Table 8-4 describes the contents of the top-level MIB object groups.

Table 8-4. Contents of Top-Level MIB Objects

Top-Level MIB Object Group	Types of Objects and 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
wfLine	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
rptrBasicPackage	Repeater configuration, status, and control information	Repeater operational state
rptrMonitorPackage	Objects that monitor repeater performance statistics	Performance and error statistics for groups and ports
rptrAddrTrackPackage	Table of address mapping information about the repeater ports	Source address of the last readable frame that the port received

Getting Instances of MIB Objects

You can select and retrieve instances for as many as 10 MIB objects at one time.

To locate individual objects:

1. **In the Statistics Manager window, choose Tools > Quick Get.**

   The Quick Get Facility window opens (refer to Figure 8-23).

2. **Select the top-level object group to which the objects belong (refer to Table 8-4).**

   The MIB Objects list displays the subordinate groups. For example, when you select wfApplication, the objects shown in Figure 8-23 appear.

3. **Select additional object groups until you reach the individual objects you want.**

   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 in the wfIpInterfaceTable group.

4. **Select each object whose statistics you want to display (selectable objects are indented).**

   When you select an individual object, the Object Information box 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

   a. **Click on Read Description in the Object Information box to display a Statistics Help window that contains a more detailed description of the object.**

   b. **Click on OK to exit the Statistics Help window.**

   To deselect an object in the MIB Objects list, click on the object again.

Formatting the MIB Object Information Display

To specify the format of MIB objects retrieved in the Output box (bottom of the Quick Get Facility window), use the Display Information and Retrieval Filter fields of the Quick Get Facility window.

You can format the output MIB object information as follows:

- Display all instances of selected MIB objects with or without their instance IDs.
- Display specific instances of selected MIB objects with or without their instance IDs.

To format the MIB object Output display:

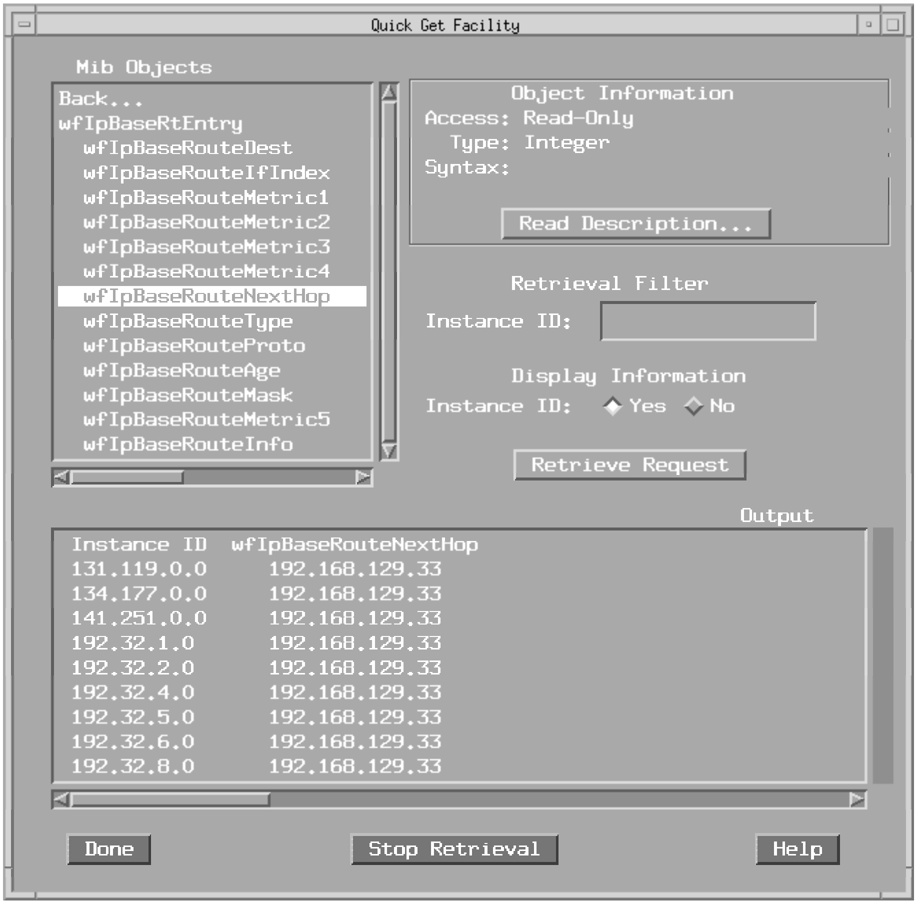
1. **In the Quick Get Facility window, set the Retrieval Filter and Display Information fields according to Table 8-5.**

Table 8-5. Retrieval Filter and Display Information Field Settings

MIB Object Output Display	Retrieval Filter	Display Information
All instances of selected MIB objects with instance IDs	Leave blank	Yes
All instances of selected MIB objects without instance IDs	Leave blank	No
Specific instances of MIB objects with instance IDs	Enter all or part of the instance ID for the MIB object, for example, 192.168.	Yes
Specific instances of MIB objects without instance IDs	Enter all or part of the instance ID for the MIB object, for example, 192.168.	No

2. **Click on Retrieve Request.**

   The Quick Get Facility displays the list of instances of the selected MIB objects in the Output box. Figure 8-25 shows all instances with their instance IDs; Figure 8-26 shows all instances without their instance IDs.



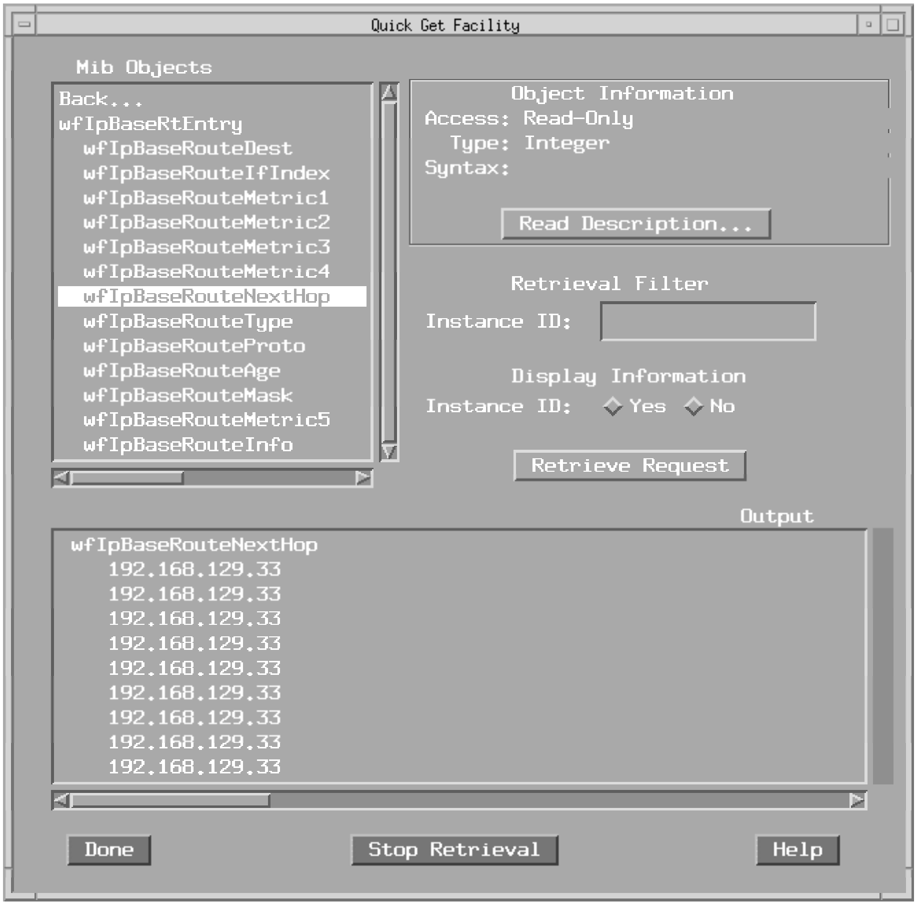
Access: Read-Only
Type: Integer
Syntax:

Instance ID:

Instance ID: ◆ Yes ◇ No

```
Instance ID  wfIpBaseRouteNextHop
131.119.0.0     192.168.129.33
134.177.0.0     192.168.129.33
141.251.0.0     192.168.129.33
192.32.1.0      192.168.129.33
192.32.2.0      192.168.129.33
192.32.4.0      192.168.129.33
192.32.5.0      192.168.129.33
192.32.6.0      192.168.129.33
192.32.8.0      192.168.129.33
```

Figure 8-25. Quick Get Facility Window: All MIB Objects with Instance IDs



```
Back...
wfIpBaseRtEntry
  wfIpBaseRouteDest
  wfIpBaseRouteIfIndex
  wfIpBaseRouteMetric1
  wfIpBaseRouteMetric2
  wfIpBaseRouteMetric3
  wfIpBaseRouteMetric4
  wfIpBaseRouteNextHop
  wfIpBaseRouteType
  wfIpBaseRouteProto
  wfIpBaseRouteAge
  wfIpBaseRouteMask
  wfIpBaseRouteMetric5
  wfIpBaseRouteInfo
```

Access: Read-Only
Type: Integer
Syntax:

Instance ID:

Instance ID: ◇ Yes ◇ No

```
wfIpBaseRouteNextHop
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
   192.168.129.33
```

Figure 8-26. Quick Get Facility Window: All MIB Objects Without Instance IDs

If you specified specific instances and not all instances, the Quick Get Facility window would show a display similar to Figures 8-25 and 8-26, with the Instance ID field completed and only the specific instances in the Output box.

3. **Click on Stop Retrieval to halt the retrieval of objects.**

4. **Click on Retrieve Request to refresh the display in the Output field.**

5. **Click on Done to exit the Quick Get Facility window.**

   You return to the Statistics Manager window.

Using the ASCII Version of the Bay Networks MIB

Site Manager software provides a directory of ASCII MIB files in ASN.1 syntax -- each file (identified by a *.mib* extension) contains a single MIB. You can use these files as a reference to MIB objects. You can also compile these files with a network management application to provide network management access to Bay Networks routers.

MIB files are found in the Windows directory *\wf\mibs* or the UNIX directory */usr/wf/mibs*. For example, the Point-to-Point Protocol MIB (ppp) can be found in */usr/wf/mibs/ppp.mib* on a UNIX workstation, or in *\wf\mibs\ppp.mib* on a PC.

Using the MIB II Counters Feature

MIB II is the second version of the Management Information Base. The MIB II Counters feature lets you track the number of packets each circuit in the router processes at the data link layer. By default, Site Manager enables the MIB II counters described in Table 8-6.

Table 8-6. MIB II Counters

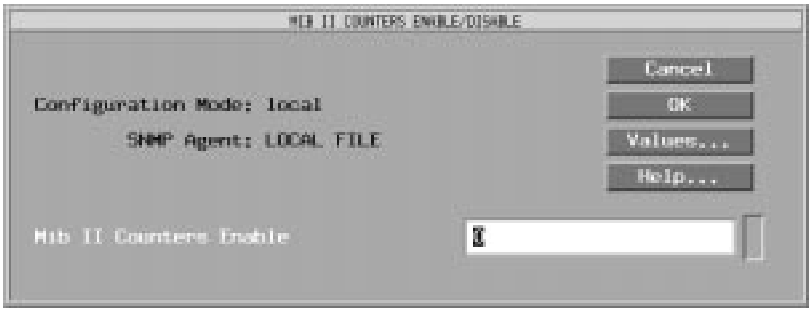
Counter	Description
ifInNUcastPkts	Counts the number of non-unicast (such as subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol
ifOutUcastPkts	Counts the total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
ifOutNUcastPkts	Counts the total number of packets that higher-level protocols requested be transmitted to a non-unicast address, including those that were discarded or not sent
ifInUcastPkts	Counts the number of subnetwork-unicast packets delivered to a higher-layer protocol
ifInUnknownProtos	Counts the number of packets received by the interface that were discarded because of an unknown or unsupported protocol

To access these counters in the MIB Browser, use the Quick Get tool to select the objects *wfApplication*, *wfDataLink*, *wfIfGroup*, and then *wfIfTable*.

By default, the MIB II counters are enabled. To measure packet count statistics accurately, you should not disable the counters; doing so would result in inaccurate aggregate statistics. However, if you choose to disable the counters, you can do so by following these steps:

1. **In the Configuration Manager window, choose Platform > MIB II Counters.**

   The MIB II Counters Enable/Disable window opens (Figure 8-27).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Mib II Counters Enable

Figure 8-27. MIB II Counters Enable/Disable Window

2. **Select Disable for the MIB II Counters Enable parameter.**

   Note that disabling the counters disables them on all circuits and slots. Likewise, enabling the counters enables them on all circuits and slots.

3. **Click on OK to save the change.**

   You return to the Configuration Manager window.

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 9
Examining Configuration File Reports

The Report Generator creates a report of an existing configuration file; it does not record changes as they are made to the file, only the file's existing contents. The Report Generator creates a report by translating 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.

The configuration file is difficult to read by looking through Site Manager configuration windows. Using the Report Generator, you receive a report that is easy to read and useful for cross-referencing information against another router's configuration report. It is a helpful tool for troubleshooting your router's configuration.

This chapter contains the following information:

If you are running Site Manager on a UNIX workstation, you can convert your ASCII configuration file reports into bootable binary configuration files (refer to "Generating Binary Configuration Files" on page 9-11.

Generating Configuration File Reports

You can generate reports from a router's configuration file from

- 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:

1. **In the main Site Manager window, choose Tools > Report Generator.**

   The Configuration Report Generator window opens (Figure 9-1).

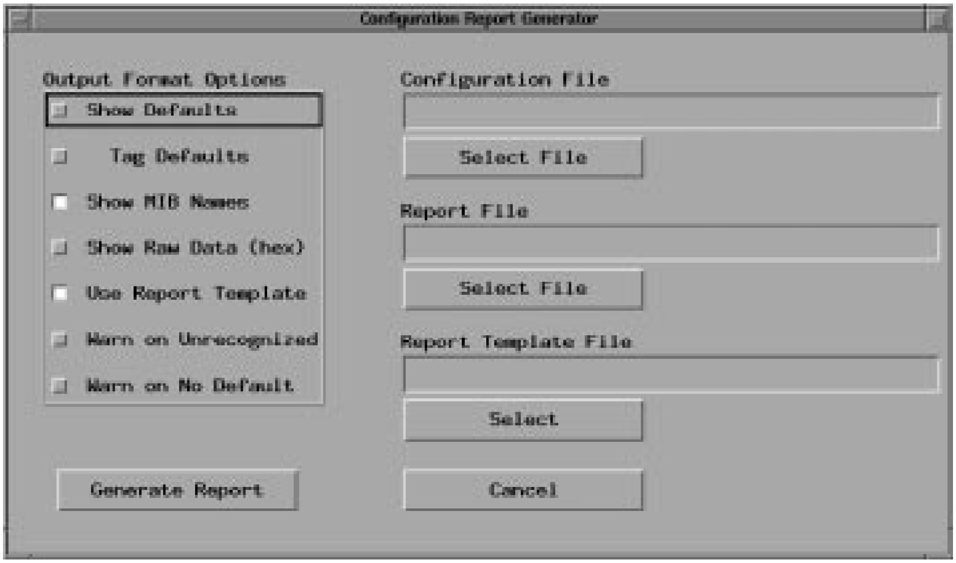


Figure 9-1. Configuration Report Generator Window

2. **In the Output Format Options box, click on the options that you want to use in the report.**

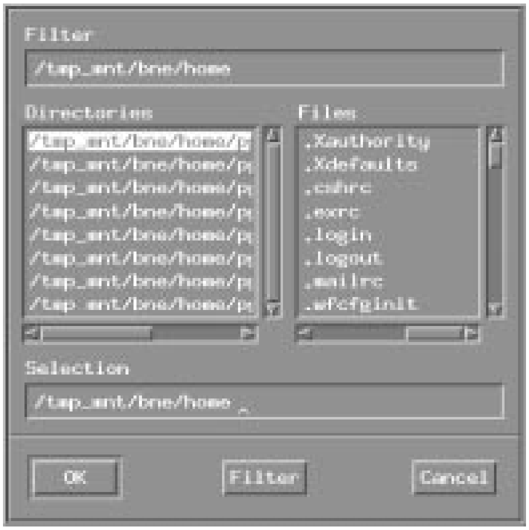
Table 9-1 describes each option.

Table 9-1. Report Generator Output Format Options

Option	Description
Show Defaults	Includes the default MIB 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 default MIB value. If you click on Tag Defaults and 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 hexadecimal configuration data along with the ASCII translation of that data. You might want to include the hexadecimal data if you plan to use the Technician Interface for configuration. In the Technician Interface, you must enter the data in raw format.
Use Report Template	Indicates that you want to use a report template other than the default. The default is a template based on the version of the configuration file. For example, the Report Generator uses a 12.0 template file to generate a report for a 12.0 configuration file. You may want to use a report template other than the configuration file version. If you select this option, the Report Template File field appears below the Report File field in the Configuration Report Generator window. You must enter a file name in the Report Template File field.
Warn on Unrecognized	Includes the warning "Unrecognized Attribute" for any attribute that is in the configuration file but is not present in the MIB.
Warn on No Default	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 default MIB value.

3. **Under the Configuration File field, click on Select File.**

The window in Figure 9-2 opens.



Filter

/tmp_mnt/bne/home

Directories

/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p

Files

.Xauthority
.Xdefaults
.cshrc
.exrc
.login
.logout
.mailrc
.wfcfginit

Selection

/tmp_mnt/bne/home

Figure 9-2. Filter Window to Select Configuration File

4. **Select the configuration file as follows:**

   a. **From the Directories list, select the directory path of the configuration file for the report.**

   b. **From the Files list, select the configuration file.**

      The path name and file name appear in the Selection field.

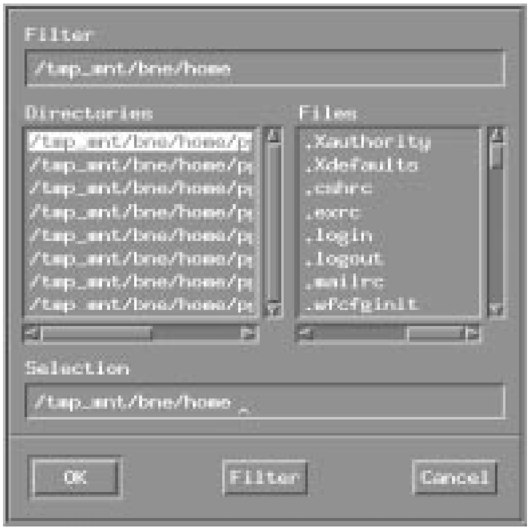
   c. **Click on OK.**

      You return to the Configuration Report Generator window.

5. **Under the Report File field, click on Select File.**

   The window in Figure 9-3 opens.

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



Filter

/tmp_mnt/bne/home

Directories

/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p
/tmp_mnt/bne/home/p

Files

.Xauthority
.Xdefaults
.cshrc
.exrc
.login
.logout
.mailrc
.wfcfginit

Selection

/tmp_mnt/bne/home

Figure 9-3. Filter Window to Save a Report File

6. **Select a location for the report file as follows:**

   a. **From the Directories list, select the directory path where you want to store the configuration file report.**

      The path appears in the Selection field.

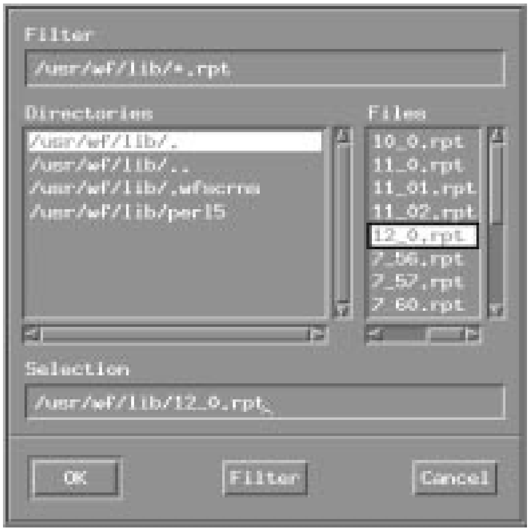
   b. **Type a file name for the report at the end of the path in the Selection field.**

   c. **Click on OK.**

      You return to the Configuration Report Generator window.

7. **If you selected Use Report Template in the Output Format Options list, under the Report Template File field, click on Select File.**

   The window in Figure 9-4 opens.



Filter

/usr/wf/lib/*.rpt

Directories

/usr/wf/lib/.
/usr/wf/lib/..
/usr/wf/lib/.wfscrns
/usr/wf/lib/perl5

Files

10_0.rpt
11_0.rpt
11_01.rpt
11_02.rpt
12_0.rpt
7_56.rpt
7_57.rpt
7_60.rpt

Selection

/usr/wf/lib/12_0.rpt

Figure 9-4. Filter Window to Select Report Template

8. **Select the report template as follows:**

   a. **From the Directories list, select the directory path that contains the template file you want to use.**

   b. **From the Files window, select the template file.**

      On UNIX workstations, the template files are in the directory */usr/wf/lib*. On the PC, the template files are in the directory *c:\wf\lib*. The format of the template file name is *<version>.rpt.*

      For example, for Version 12.00 the template is *12_0.rpt*.

      The path name and file name appear in the Selection field.

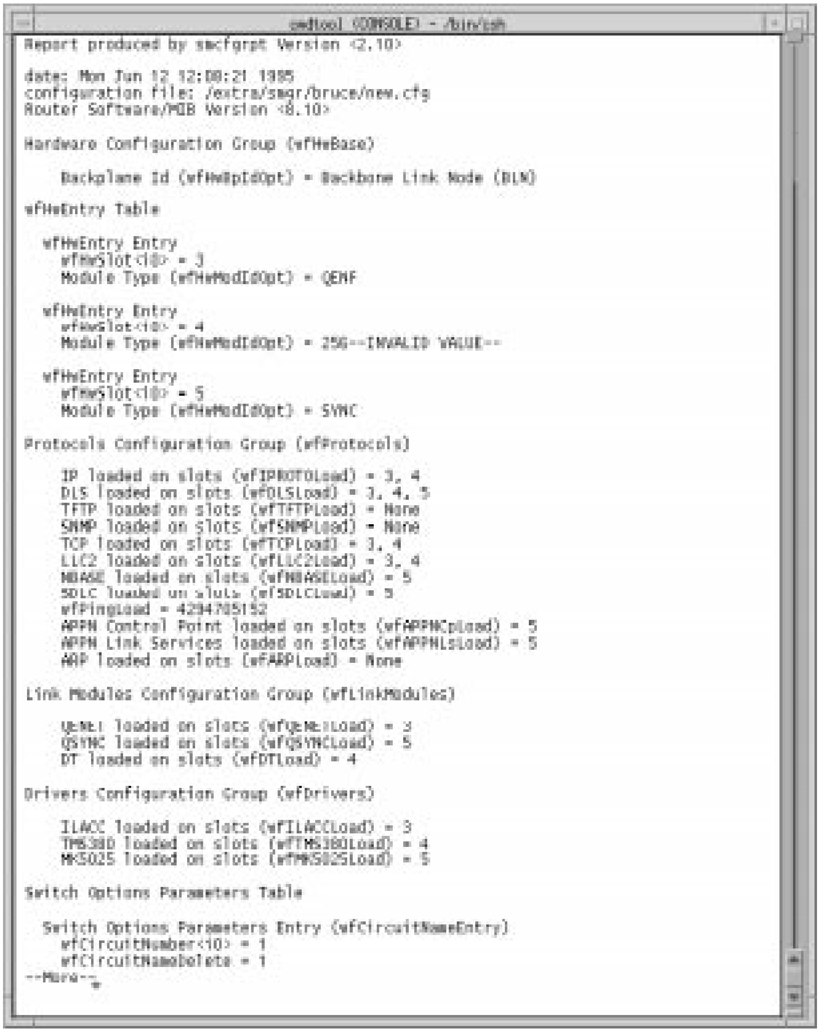
   c. **Click on OK.**

      You return to the Configuration Report Generator window.

9. **Click on Generate Report.**

   Site Manager generates the configuration file report and saves the report under the file name you specified. You can then open the report using a text editor.

Figure 9-5 shows an example of a configuration file report. This is just one portion of the entire report.



```
Report produced by smcfgrpt Version <2.10>

date: Mon Jun 12 12:08:21 1995
configuration file: /extra/smgr/bruce/new.cfg
Router Software/MIB Version <8.10>

Hardware Configuration Group (wfHwBase)

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

wfHwEntry Table

  wfHwEntry Entry
    wfHwSlot<10> = 3
    Module Type (wfHwModIdOpt) = QENF

  wfHwEntry Entry
    wfHwSlot<10> = 4
    Module Type (wfHwModIdOpt) = 256--INVALID VALUE--

  wfHwEntry Entry
    wfHwSlot<10> = 5
    Module Type (wfHwModIdOpt) = SYNC

Protocols Configuration Group (wfProtocols)

    IP loaded on slots (wfIPROTOLoad) = 3, 4
    DLS loaded on slots (wfDLSLoad) = 3, 4, 5
    TFTP loaded on slots (wfTFTPLoad) = None
    SNMP loaded on slots (wfSNMPLoad) = None
    TCP loaded on slots (wfTCPLoad) = 3, 4
    LLC2 loaded on slots (wfLLC2Load) = 3, 4
    NBASE loaded on slots (wfNBASELoad) = 5
    SDLC loaded on slots (wfSDLCLoad) = 5
    wfPingLoad = 4294705152
    APPN Control Point loaded on slots (wfAPPNCpLoad) = 5
    APPN Link Services loaded on slots (wfAPPNLsLoad) = 5
    ARP loaded on slots (wfARPLoad) = None

Link Modules Configuration Group (wfLinkModules)

    QENET loaded on slots (wfQENETLoad) = 3
    QSYNC loaded on slots (wfQSYNCLoad) = 5
    DT loaded on slots (wfDTLoad) = 4

Drivers Configuration Group (wfDrivers)

    ILACC loaded on slots (wfILACCLoad) = 3
    TMS380 loaded on slots (wfTMS380Load) = 4
    MK5025 loaded on slots (wfMK5025Load) = 5

Switch Options Parameters Table

  Switch Options Parameters Entry (wfCircuitNameEntry)
    wfCircuitNumber<10> = 1
    wfCircuitNameDelete = 1
--More--
```

Figure 9-5. Sample Configuration File Report

Notice that the report includes information about the entire configuration, hardware and software, including module types and parameter settings.

Generating Configuration File Reports from UNIX

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

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

Table 9-2 describes the options you can use in the UNIX command line.

Table 9-2. Options for Command Line (UNIX)

Option	**Description**
-d	Includes the default MIB 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 (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 template based on the version of the configuration file. Template files are in */usr/wf/lib.* The format of the template file name is *<version>.rpt, f*or example, *12_0.rpt.*
-c <*configuration file*>	Specifies the name of the configuration file from which you want to generate a report
-o <*report file*>	Specifies the path and file name of the report file. If you omit this argument, the Report Generator sends the output to *<stdout>.*

Generating Configuration File Reports from Windows

To generate a configuration file report from Windows 95 on a PC:

1. **From the Windows desktop, choose Start > Programs > MS-DOS prompt.**

   The DOS window opens.

2. **At the DOS prompt, go to the \*wf* directory.**

3. **Enter the smcfgrpt command in the following format:**

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

   Table 9-3 describes the options you can use in this command line.

4. **Click on OK.**

   The Report Generator generates a configuration file report.

Table 9-3. Options for Command Line (Windows)

Option	**Description**
-d	Includes the default MIB 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 (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 template based on the version of the configuration file. Template files are in *c:\wf\lib*. The format of the template file name is *<version>.rpt,* for example, *12_0.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 path name.
-o *<report file>*	Specifies the path name of the report file

Generating Binary Configuration Files

If you are running Site Manager on a UNIX workstation, you can use Config Generator (rpt2cfg), a UNIX command-line tool, to create bootable binary configuration files from your edited ASCII configuration file reports. Config Generator creates configuration files faster than the Configuration Manager.

Make sure you are familiar with the ASCII configuration file format and know exactly what changes to make before you use Config Generator. For additional information or advice, contact the Bay Networks Technical Solutions Center.

Caution: Use Config Generator only if you are an experienced user. It provides very limited validation checking of the edited ASCII configuration file. If you attempt to boot from a corrupt configuration file, the results will be unpredictable. The router or platform may fail diagnostics or fail to boot.

To create a bootable binary configuration file with Config Generator you need to

- Use the Report Generator to create an ASCII configuration file report. Refer to “Generating Configuration File Reports” on page 9-2.
- Use a text editor to make changes to the file.
- Use Config Generator to convert the edited ASCII configuration file report to a bootable binary configuration file.

Preparing the ASCII Configuration File

To use Config Generator you must include the Bay Networks MIB names in the ASCII configuration file report that you create using the Report Generator. If you exclude MIB names, Config Generator cannot create a valid binary file.

Choose the appropriate option when you generate your report:

- If you are using the Report Generator from Site Manager, select the Show MIB Names option in the Output Format Options box in the Configuration Report Generator window.
- If you are using the Report Generator from the UNIX or Windows command line, use the **-m** option.

You can select any of the other options you want to include in the ASCII configuration file report, as long as you include the MIB names.

Using Config Generator

Config Generator is available to users of Site Manager Version 4.0 or later. Config Generator is located in the */usr/wf/bin* directory, along with the other Site Manager command-line tools.

You run Config Generator from the UNIX command line. Enter the name of the edited ASCII configuration file you want to convert and a name for the new binary configuration file in the following format:

rpt2cfg -f *<ASCII Report Filename>* [**-o** *<New Binary Filename>*]

If you do not supply a new binary file name, Config Generator sends the output to *<stdout>*.

Depending on the size of the file, Config Generator may take several minutes to convert the file. When Config Generator is finished, the UNIX prompt returns. If no error messages appear, Config Generator created and saved the binary configuration file. If you receive an error message, the file is corrupt and should not be used.

Checking for Errors

Config Generator checks the ASCII configuration file for valid MIB names, valid MIB values, and for duplicate circuit names. If these errors are found, Config Generator displays the line number in the ASCII configuration file where the error occurred, and a brief description of the error. The program does not check for cross-dependencies within the file.

Correct any errors in the ASCII configuration file report and run Config Generator on the corrected file. When you are satisfied that you have a valid binary configuration file, use TFTP to transfer the file to the router and reboot. (Refer to Chapter 5 for instructions.)

Remember that Config Generator provides very limited error checking. Always keep a valid binary configuration file ready in case the boot fails.

Checking MIB Attributes

You can use Config Generator to find the possible MIB attributes for a particular MIB record. To find the possible attributes, you provide the MIB name and MIB version number in the following format:

```
rpt2cfg -q <MIB Name> -d <MIB Version Number>
```

MIB Version Number is the current software version number (for example, 12.00). For example, to find the MIB attributes for Version 12.00 of the MIB record wfsys, enter the following command:

```
rpt2cfg -q wfsys -d 12.00
```

Config Generator displays the following:

```
Possible valid attributes for this record entry are:
wfSysContact
wfSysName
wfSysLocation
wfSysMibRevision
wfSysMibCounterEnable
```

Checking MIB Attribute Values

You can use Config Generator to find valid values for a given MIB attribute. To find the values, you provide the MIB attribute and the MIB version number in the following format:

```
rpt2cfg -q <MIB Attribute> -d <MIB Version Number>
```

MIB Version Number is the current software version number, for example, 12.00. For example, to find the values for Version 12.00 of the MIB attribute wfSysMibCounterEnable enter the following:

```
rpt2cfg -q wfSysMibCounterEnable -d 12.00
```

Config Generator displays the following:

```
Possible valid list of values are:
DISABLE, ENABLE
```

Identifying Files Created by Config Generator

Config Generator adds a text string to the system name of the configuration files it generates so that you can differentiate them from other configuration files.

To see the text string:

1. **In the main Site Manager window, choose Tools > Configuration Manager.**

   The Configuration Manager window opens.

2. **In the Configuration Manager window, choose Platform > Edit System Information.**

   You will see the following message in the System Name field:

   ```
   /This binary config was created using rpt2cfg
   ```

You will also see this message in any ASCII configuration file reports that you create with the Report Generator from binary configuration files that you created with Config Generator. You can see the message on the line in the file that identifies the system name.

Chapter 10
Auditing Configuration Files

In organizations where network managers at branch locations share router management responsibilities, central administrators can use audit trail logs to monitor who changes a configuration file.

The Audit Trail feature lets you record who made changes to a configuration file from a single Site Manager workstation, and then place this information in an ASCII file called an *audit trail log*. Each router has its own audit trail log and each Site Manager workstation uses the audit trail feature independently. You cannot create a log file for multiple Site Manager workstations.

Each time someone changes a configuration file, the audit trail feature, if enabled for that router, appends the changes to the audit trail log.

This chapter contains the following information:

Audit Trail Feature for Remote and Dynamic Mode

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. You must always enable the audit trail feature before it can track changes.

If you configure the router in remote mode, Site Manager does the following:

- Transfers the configuration file to the router
- Creates the audit trail log file (if it does not already exist)
- Appends the configuration changes to the audit trail log

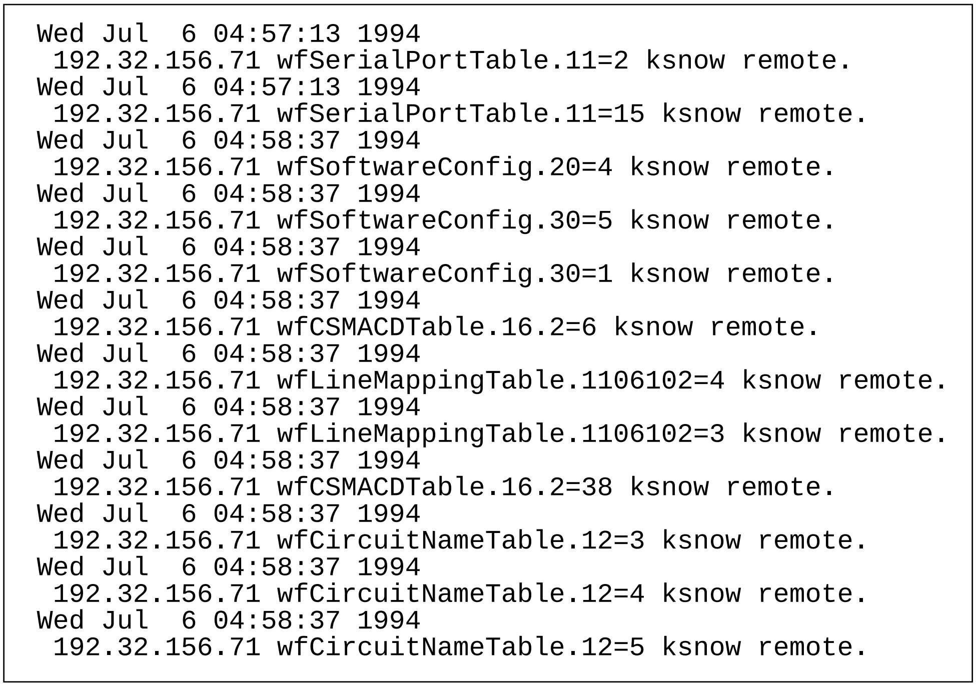
If you configure the router in dynamic mode, Site Manager does the following each time an SNMP SET occurs:

- Updates the configuration on the router
- Logs changes to a MIB object in the audit trail log, which is created if it does not already exist, and appends the changes to the file

Viewing an Audit Trail Log File

After Site Manager creates an audit trail log and appends information to it, you can open the log file, *audit.cfg*, using any standard text editor. You can also print the file.

Figure 10-1 shows a sample audit trail log.



```
Wed Jul  6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=2 ksnow remote.
Wed Jul  6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=15 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.20=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=5 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=1 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=6 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=3 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=38 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=3 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=5 ksnow remote.
```

Figure 10-1. Sample Audit Trail Log File

Maintaining an Audit Trail Log

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.

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 for the routers.
- 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

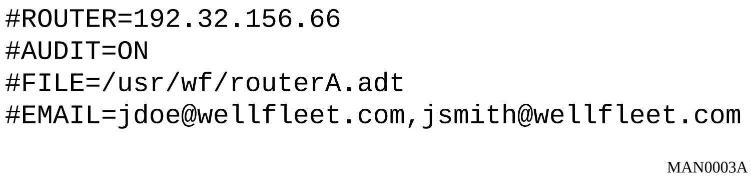
Site Manager provides a default audit trail configuration file, *audit.cfg*. The file resides in */usr/wf* on UNIX workstations, and in *c:\wf* on PCs. You must edit the file to specify the following information for each router you want to audit:

- The IP address of the router
- The path name of the audit trail log file
- The e-mail 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:

1. **On a UNIX workstation, copy the *audit.cfg* file to a directory where you have write permission.**
2. **Open *audit.cfg* using a standard text editor.**

   Figure 10-2 shows the default file.



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

Figure 10-2. 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 (#) from the beginning of all four lines.**
5. **In the first line, ROUTER=, overwrite the default value with the IP address of the router you want to audit.**
6. **In the FILE= line, overwrite the default value with the path name and file name 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 file name should be the router's name (not its IP address) followed by the *.adt* extension. For example:

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

7. **In the EMAIL= line, overwrite the default value with the e-mail addresses of users you want to notify of configuration changes.**

   Use a comma to separate each e-mail address, for example:

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

   If you do not want to use mail notification, delete the default e-mail addresses.

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

8. **In the AUDIT= line, accept the default value, ON, to enable the feature.**

   To disable the audit trail log, type **OFF**.

9. **Repeat steps 2 through 8 for each router that you want to audit.**
10. **Save your changes and exit the file.**

Modifying the Audit Path Environment Variable

You must specify the new path name 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

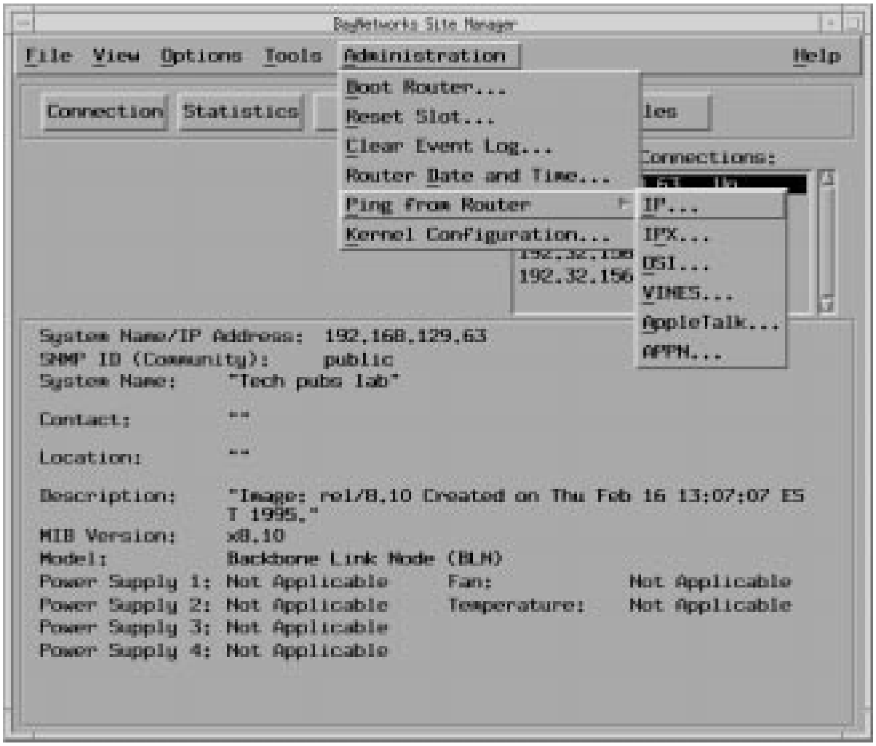
Chapter 11
Using the Ping Option

The Site Manager Ping from Router option lets you test whether the router can contact other remote devices. The ping option works with the IP, IPX, OSI, VINES, AppleTalk, and APPN protocols.

This chapter contains the following information:

Checking Router Connections Using Ping

To ping other remote devices from the router, choose Administration > Ping from Router in the Site Manager window and then choose one of the protocols listed in the menu (Figure 11-1).



```
System Name/IP Address:  192.168.129.63
SNMP ID (Community):     public
System Name:       "Tech pubs lab"

Contact:           ""

Location:          ""

Description:       "Image: rel/8.10 Created on Thu Feb 16 13:07:07 ES
                   T 1995."
MIB Version:       x8.10
Model:             Backbone Link Node (BLN)
Power Supply 1:  Not Applicable      Fan:              Not Applicable
Power Supply 2:  Not Applicable      Temperature:      Not Applicable
Power Supply 3:  Not Applicable
Power Supply 4:  Not Applicable
```

Figure 11-1. Ping from Router Menu

The following sections describe the available ping options.

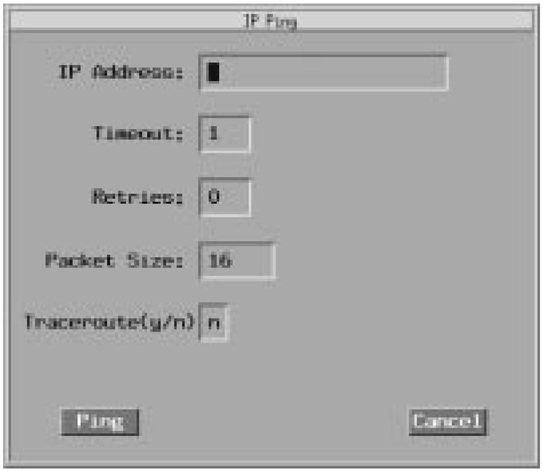
IP Ping

When you ping a remote device using IP, the ping program residing on the router sends an Internet Control Message Protocol (ICMP) echo request to the remote address you specify in the IP Ping window. The remote device responds to the router's request if it can be reached. A window then opens showing the response or the result of the request.

To ping a remote device running IP:

1. **In the main Site Manager window, choose Administration > Ping from Router > IP.**

   The IP Ping window opens (Figure 11-2).



IP Address:

Timeout: 1

Retries: 0

Packet Size: 16

Traceroute(y/n) n

Figure 11-2. IP Ping Window

2. **In the IP Address field, type the IP address of the remote device.**
3. **In the Timeout field, type the number of seconds after which the ping should time out.**

   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, type 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.

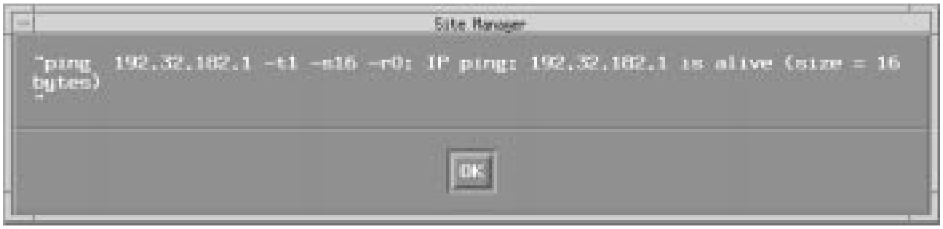
5. **In the Packet Size field, type the number of bytes of data to send with each ping.**
6. **In the Traceroute field, type y (yes) if you want the router to generate a path report that shows the intervening hop addresses to the destination.**
7. **Click on Ping.**

IP Ping Responses

Site Manager displays one of the following messages when you click on 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

  An “alive” message appears if the router received an ICMP echo response from the target device within the timeout period. The message also provides the size of the test packet. Figure 11-3 shows a sample message.

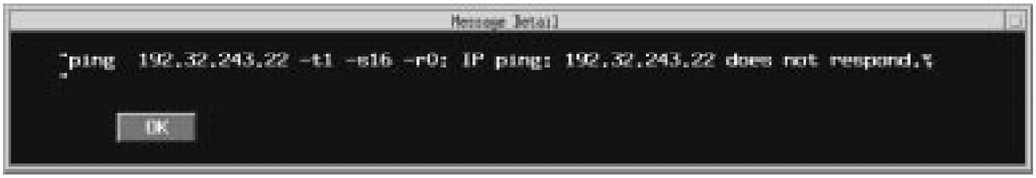


```
"ping  192.32.182.1 -t1 -s16 -r0: IP ping: 192.32.182.1 is alive (size = 16
bytes)
"
```

Figure 11-3. Ping Is Alive Window

- A “does not respond” message

  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 period. Figure 11-4 shows a sample message.



```
"ping  192.32.243.22 -t1 -s16 -r0: IP ping: 192.32.243.22 does not respond.%
"
```

Figure 11-4. Ping Does Not Respond Window

- An “ICMP host unreachable from <*y.y.y.y*>” message

  An “ICMP host unreachable from <*y.y.y.y*>” message appears if the router whose address is *y.y.y.y* cannot forward the ping request any further along the path to the target device. IP updates its IP routing or Address Resolution Protocol (ARP) table accordingly. A sample message follows:

  ```
  ping: ICMP host unreachable from 192.32.243.1
  ```

- A target address “is unreachable” message

  A target address “is unreachable” message appears if the router previously issued an “ICMP host unreachable from <*y.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, the device responds if it can be reached, and Site Manager displays the response or the result of the request.

IPX configuration request packets are typically used to get configuration information from other devices on a NetWare 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 0xFFFFFFFFFFFF (broadcast host destination)

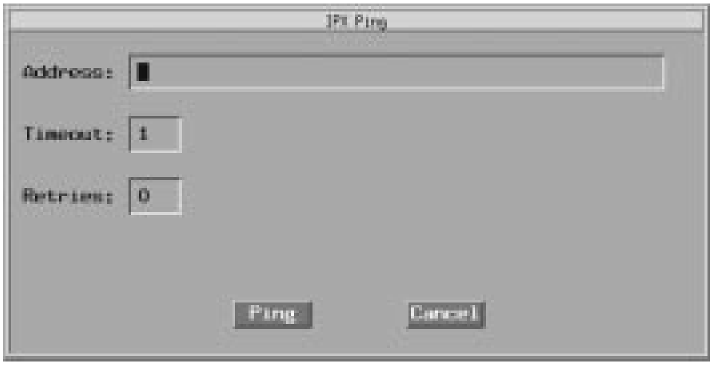
The IPX router will only respond to request packets sent directly to one of its interface addresses. If you send a request packet from a router to an IPX interface on that same router, the router does not send the request packet out onto the line. Instead, the router sends the packet internally to the specified interface, which then responds internally.

Note: The IPX router will respond (reply with a ping response) to any ping packet that comes in on socket number 9086 and that has a type field of 0.

To send an IPX configuration request packet:

1. **In the main Site Manager window, choose Administration > Ping from Router > IPX.**

   The IPX Ping window opens (Figure 11-5).



IPX Ping

Address:

Timeout: 1

Retries: 0

Figure 11-5. IPX Ping Window

2. **In the Address field, type 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, type the number of seconds after which each ping times out.**

   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, type the number of successive times the router should repeat the ping.**

   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, for example:

  ```
  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 period, for example:

  ```
  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 period, for example:

  ```
  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, for example:

  ```
  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, for example:

  ```
  IPX ping: resource error
  ```

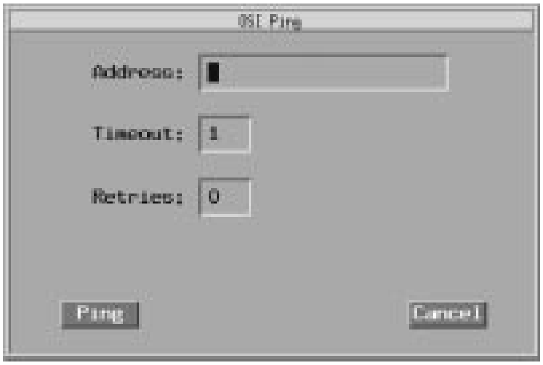
OSI Ping

When you issue an Open Systems Interconnection (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.

To send a CLNP echo request:

1. **In the main Site Manager window, choose Administration > Ping from Router > OSI.**

   The OSI Ping window opens (Figure 11-6).



OSI Ping

Address:

Timeout: 1

Retries: 0

Figure 11-6. OSI Ping Window

2. **In the Address field, type the NSAP address of the remote device in hexadecimal notation.**
3. **In the Timeout field, type the number of seconds the router should wait for a response from the remote device.**

   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, type 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.
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 a message 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 period, for example:

  ```
  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, for example:

  ```
  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 period, for example:

  ```
  OSI ping: 49000400000a12121200 does not respond
  ```

- An “NSAP address is too short” message appears if the NSAP address is too short. The allowed NSAP address length is 20 hexadecimal characters (10 bytes), for example:

  ```
  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, for example:

  ```
  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, for example:

  ```
  OSI ping: resource error
  ```

- A “system error” message appears if the Technician Interface fails, for example:

  ```
  OSI ping: system error
  ```

- A “<*y.y.y.y.y.y.y.y.y.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 characters.

  y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y is the address of the CLNP host.

  For example:

  ```
  OSI ping: 123456Z is a bad NSAP address
  ```

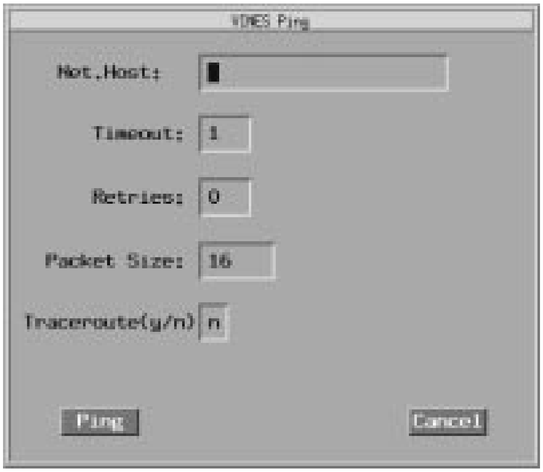
VINES Ping

When you issue a VINES ping to a remote VINES device, the router responds if the device can be reached. Site Manager displays the response.

To send a VINES request to determine the network connectivity of a VINES host:

1. **In the main Site Manager window, choose Administration > Ping from Router > VINES.**

   The VINES Ping window opens (Figure 11-7).



Net.Host:

Timeout: 1

Retries: 0

Packet Size: 16

Traceroute(y/n) n

Figure 11-7. VINES Ping Window

2. **In the Net. Host field, type 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 that 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, type the number of seconds after which each ping times out.**

   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, type 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.

5. **In the Packet Size field, type the number of bytes of data to send with each ping.**

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.**

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 other than 0 for Retries, Site Manager displays a message 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 period. The message also indicates the size of the test packet, for example:

  ```
  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 period, for example:

  ```
  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, for example:

  ```
  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, for example:

  ```
  VINES ping: resource error
  ```

- An “invalid parameter specified” message appears if you specify an invalid parameter when you issue a VINES ping, for example:

  ```
  VINES ping: invalid parameter specified
  ```

- A “VINES service is not running” message appears if the VINES service is not enabled on the router, for example:

  ```
  VINES ping: VINES service is not running
  ```

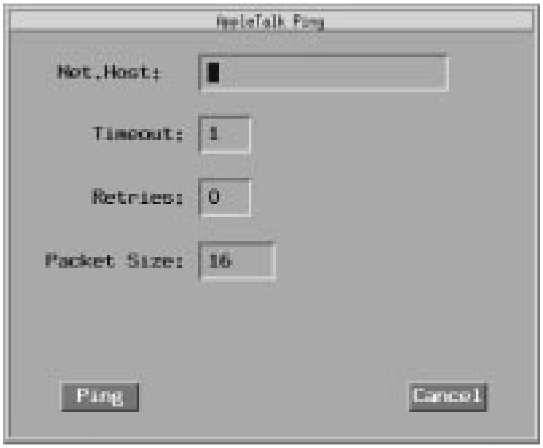
AppleTalk Ping

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:

1. **In the main Site Manager window, choose Administration > Ping from Router > AppleTalk.**

   The AppleTalk Ping window opens (Figure 11-8).



Net.Host:

Timeout: 1

Retries: 0

Packet Size: 16

Figure 11-8. AppleTalk Ping Window

2. **In the Net.Host field, type 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, type the number of seconds after which each ping times out.**

   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, type 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.

5. **In the Packet Size field, type the number of bytes of data to send with each ping.**

   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 other than 0 for Retries, Site Manager displays a message 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 period. The message also indicates the size of the test packet, for example:

  ```
  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 period, for example:

  ```
  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, for example:

  ```
  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, for example:

  ```
  AppleTalk ping: resource error
  ```

- An “invalid parameter specified” message appears if you specify an invalid parameter when you issue an AppleTalk ping, for example:

  ```
  AppleTalk ping: invalid parameter specified
  ```

- An “AppleTalk service is not running” message appears if the AppleTalk service is not enabled on the router, for example:

  ```
  AppleTalk ping: Appletalk service is not running
  ```

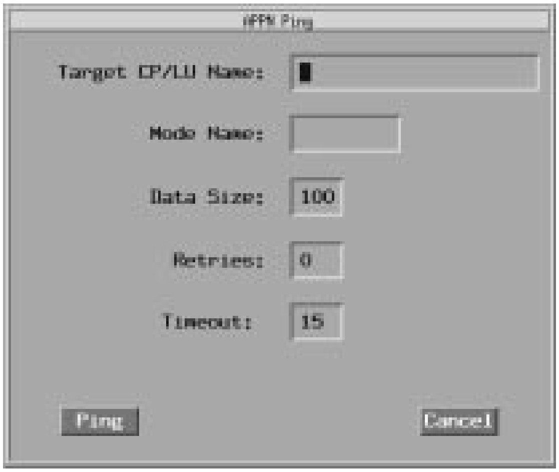
APPN Ping

When you issue an APPN ping to a remote APPN device, the remote device responds if it can be reached, and Site Manager displays the response or the result of the request. APPN ping uses the APING (APPN Ping) Transaction Program (TP) to send an APING request to the APING TP running on the remote device.

To send an APPN ping request:

1. **In the main Site Manager window, choose Administration > Ping from Router > APPN.**

   The APPN Ping window opens (Figure 11-9).



Target CP/LU Name:

Mode Name:

Data Size: 100

Retries: 0

Timeout: 15

Figure 11-9. APPN Ping Window

2. **In the Target CP/LU Name field, type the APPN address of the remote device.**

   Enter the address in the format of a Control Point name.

   Use the format <*network ID*>.<*CP name*> if the remote device is not on the same network as the router.

3. **In the Mode Name field, optionally type one of the following values:**

   - #INTER for interactive mode, for example, when there is not much data involved and response time is very important
   - #BATCH for batch-like mode, when there is a lot of data involved and response time is not important
   - #INTERSC for a secure version of the interactive mode
   - #BATCHSC for a secure version of the batch-like mode

   You can leave this field blank to use the default mode, which is similar to #INTER.

   APPN route calculation uses the mode characteristics when determining the optional route. Specifying a mode for the ping will test whether a route exists that is suitable to carry the type of traffic that the mode identifies.

4. **In the Data Size field, type the number of bytes of data to send with each ping.**

5. **In the Retries field, type 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.

6. **In the Timeout field, type the number of seconds after which each ping times out.**

   If the router receives a response to a ping after it has timed out, it does not send an “alive” message to Site Manager.

7. **Click on Ping.**

APPN Ping Responses

Site Manager displays one of the following messages when you issue an APPN ping; Site Manager displays only one message, regardless of the number of retries you specified.

- An “alive” message appears if the router receives a response from the target device within the timeout period, for example:

  ```
  APPN ping: bay is alive
  ```

- A “did not complete in the time allowed” message appears if the node is alive but congested, the data transfer time exceeded the timeout period, or the directory search is not complete, for example:

  ```
  APPN ping: ping of bay did not complete in the time allowed
  ```

- An “unreachable” message appears if no route could be calculated to the remote device, or if the remote device does not support APING, for example:

  ```
  APPN ping: bay is unreachable
  ```

- An “invalid name” message appears if the specified node name or mode name is invalid, for example:

  ```
  APPN ping: invalid name specified
  ```

- An “APPN service is not running” message appears if the APPN service is not enabled on the router, for example:

  ```
  APPN ping: APPN service is not running
  ```

Monitoring Network Activity Using the Ping MIB

You can track network availability and response time using the ping MIB. The ping MIB supports IP ping requests only. The ping MIB is a group of tables that stores 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

You work with the ping MIB as a diagnostic tool, which distinguishes it from the Ping from Router option described in “Checking Router Connections Using Ping” on page 11-2.

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 can also create your own application to query the ping MIB, analyze the data, and generate reports of the information.

In addition to the Statistics Manager, you can use applications such as IBM NetView/6000, SunNet Manager, and HP OpenView to work with the ping MIB.

To use the ping MIB to track network availability and response time, you must:

- Configure IP ping requests.
- Review IP ping statistics.

The sections that follow explain how to do this.

Configuring IP Ping Requests

The ping MIB supports IP ping requests only.

To configure the ping requests and store the results in the ping MIB:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Tools > Configuration Manager > Local File, Remote File, or Dynamic.**

   Refer to Chapter 2 for information about opening a configuration file.

3. **In the Configuration Manager window, choose Platform > Ping at Intervals > IP.**

   The Ping at Intervals window opens (Figure 11-10).

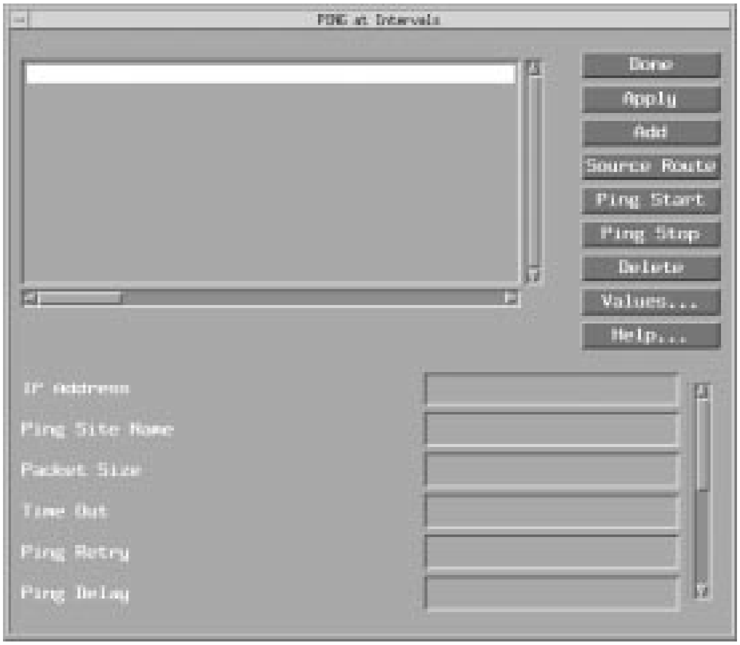
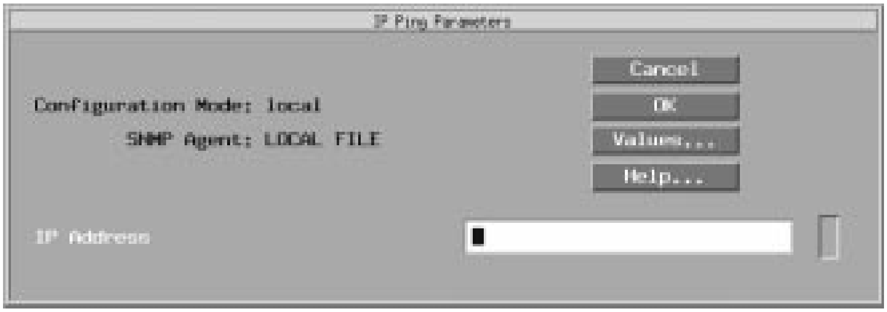


Figure 11-10. Ping at Intervals Window

4. **Click on Add.**

   The IP Ping Parameters window opens (Figure 11-11).



Configuration Mode: local
SNMP Agent: LOCAL FILE
IP Address

Figure 11-11. IP Ping Parameters Window

5. **Type the IP address that you want to ping, then click on OK.**

   You return to the Ping at Intervals window.

6. **Select the IP address for which you want to configure the ping request.**
7. **Specify values for the parameters in the Ping at Intervals window.**

   Refer to the parameter descriptions beginning on page B-17 or click on Help.

8. **Click on Apply.**
9. **If you are working in dynamic mode, click on Ping Start.**

   The router pings the IP address at the interval you specified.

   Site Manager stores the results of the ping requests in the ping MIB tables.

10. **Repeat steps 4 through 9 to configure ping requests for additional IP addresses.**

    To stop trying an address, select the address in the Ping at Intervals window and click on Ping Stop.

Deleting Ping Requests

To remove the results of a ping request from the ping MIB:

1. **In the Ping at Intervals window, select the ping request you want to delete.**
2. **Click on Delete.**
3. **Click on Apply.**
4. **Click on Done.**

   Site Manager removes all entries for the selected request from the appropriate tables. You return to the Configuration Manager window.

Specifying Source Routes for Ping Requests

If you want to use strict or loose source routing for the ping request, you must set the Source Route parameter to the appropriate value in the Ping at Intervals window (refer to Figure 11-10), then specify the routes that you want to use.

To specify source routes:

1. **In the Ping at Intervals window, click on Source Route.**

   The Source Route Entries window opens (Figure 11-12).

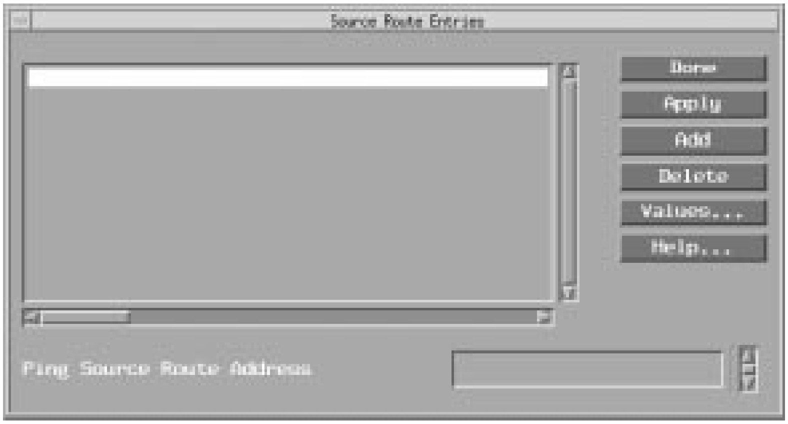
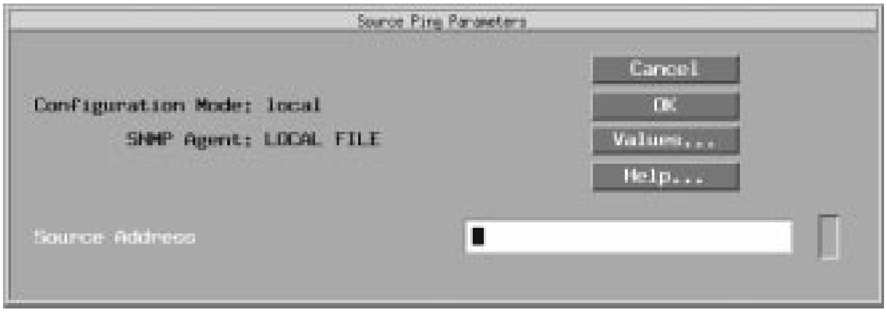


Figure 11-12. Source Route Entries Window

2. **Click on Add.**

   The Source Ping Parameters window opens (Figure 11-13).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Figure 11-13. Source Ping Parameters Window

3. **In the Source Address field, type the IP address of the first device you want to ping.**

4. **Click on OK.**

   You return to the Source Route Entries window. The IP address you just entered appears in the list.

5. **To enter additional source route addresses, repeat steps 2 through 4.**

   You can enter as many as eight source route addresses. Be sure to enter the source route addresses in the order that you want the packet to traverse them (from source to destination).

6. **Click on Apply.**

7. **Click on Done.**

   You return to the Ping at Intervals window.

Changing or Deleting Source Route Addresses

To change an IP address in the Source Route Entries window:

1. **In the Ping at Intervals window, click on Source Route.**

   The Source Route Entries window opens (refer to Figure 11-12).

2. **Click on the address in the list you want to change or delete.**

   The address appears in the Ping Source Route Address field.

3. **Do one of the following:**

   - Enter the new address in place of the old one.
   - Click on Delete to remove the entry.

     Site Manager removes the entry from the Source Route Entries window and from the ping MIB tables.

4. **Click on Apply.**

5. **Click on Done.**

   Your changes are saved and you return to the Ping at Intervals window.

   To save your changes without exiting the window, click on Apply.

Reviewing IP Ping Statistics

You can view the information in the ping MIB using the Statistics Manager. The Statistics Manager provides four default windows that contain information from the ping MIB (Table 11-1).

Table 11-1. Default Ping MIB Statistics Windows

Window Name	Contains Information from
pingmain.dat	Main ping MIB table
pinghist.dat	Ping history table
pingsrc.dat	Ping source route table
pingtrc.dat	Ping trace route table

Refer to Chapter 8 for information about retrieving 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):

1. **In the Ping at Intervals window, select the IP address of the device whose ping information you want to remove.**
2. **Click on Delete.**
3. **Click on Done.**

   You return to the Configuration Manager window.

Appendix A
Operating Site Manager with UNIX Commands

You can start Site Manager and access most Site Manager tools directly from the command line on a UNIX workstation. You cannot use the command-line options to start the Image Builder tool. Instead, at the command line, type **builder** to start the tool.

Bay Networks recommends that only experienced Site Manager operators use the command line to operate Site Manager.

Table A-1 lists the commands for starting Site Manager tools from the UNIX command line.

Table A-1. Site Manager Startup Commands

Command	Function
wfsm	Starts Site Manager
wfcfg	Starts the Configuration Manager
wflog	Starts the Events Manager
wftraps	Starts the Trap Monitor
wfrfs -a *<SNMP_agent_IP_address>*	Starts the Router Files Manager and establishes a connection with the router
wfstats -a *<SNMP_agent_IP_address>*	Starts the Statistics Manager and establishes a connection with the router
wflaunch -a *<SNMP_agent_IP_address>*	Displays an individual statistics window

You can include options in the startup command line to override Site Manager default settings. Table A-2 describes the available options.

Table A-2. Site Manager Startup Command Options

Startup Option	Startup Commands	Function	Default Setting	Example
-c <SNMP community>	All	Specifies the SNMP community string	public	**wfsm -c Sitemgr**
-a <SNMP agent IP address>	Mandatory for **wfrfs**, **wfstats**, and **wflaunch**. Use with other commands when you want to connect to a router.	Specifies the SNMP agent's IP address	none	**wfstats -a 192.32.4.2**
-m <SNMP MIB definitions file>	All	Specifies the MIB definitions file in the path */usr/wf/lib*	WFMIB.defs	**wfcfg -m mymib.defs**
-r <SNMP retry count>	All	Specifies the number of SNMP retries	3	**wflog -r 5**
-t <SNMP timeout>	All	Specifies the number of seconds for the SNMP timeout	5	**wflog -t 10**
-s <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 */etc/services*	0	**wftraps -s 161**

(continued)

Table A-2. Site Manager Startup Command Options *(continued)*

Startup Option	Startup Commands	Function	Default Setting	Example
-e <SNMP trap port>	**wfsm** **wftraps**	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 */etc/services*.	0	**wftraps -e 161**
-v <config volume>	**wfsm** **wfcfg**	Specifies the volume for remote configuration file access	2	**wfsm -v 3**
-f </path/> <file>	**wfcfg** **wflaunch**	Specifies the configuration or statistics screen file name	2	**wfcfg -f /wf/file.cfg**
-o <config mode>	**wfcfg**	Specifies the configuration mode: local, remote, or dynamic	local	**wfcfg -o remote**
-p	**wflaunch**	Displays an individual statistics window in preview mode (without displaying data)	10	**wflaunch -a 192.32.4.2 - p 1**

To start a Site Manager tool from the UNIX command line:

1. **Access an X window on your UNIX workstation.**
2. **Type one of the commands from Table A-1 and the command options you want from Table A-2.**
3. **Append the command with a space and an ampersand (&).**

   This action ensures that you can continue to enter commands in the command-line window while the tool is open.

Example

You can type 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 -t 10 &
```

The Configuration Manager window opens, displaying the IP address of the router you specified.

Appendix B
Site Manager Parameters

You can modify many configuration parameters to set up Site Manager operation, for example, the router connections parameters, system information parameters, and boot parameters. This appendix contains the parameters that you can modify.

When you configure parameters in Site Manager windows, you are modifying attributes in the Bay Networks MIB.

For each parameter, the descriptions include information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify 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*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Router Connection Options Parameters

This section describes the parameters in the Router Connection Options window.

Parameter: **Node Name/IP Address**

Default: None

Options: Valid host name or valid IP address

Function: Specifies the host name or IP address of the Bay Networks router with which you want to establish a management session. The IP address you enter becomes the default router connection address. When you open a Site Manager tool and choose Options > Router Connection, the Router Connection Options window displays this address.

Instructions: Enter the host name or IP address of the router. You can use the host name to establish a management session only if it is included in the workstation's host file.

MIB Object ID: None

Parameter: **Identity (Community)**

Default: Public

Options: Any valid SNMP community name

Function: Specifies the SNMP community name you want Site Manager to use when communicating with the router.

Instructions: Enter the SNMP community name. If you want to use the Configuration Manager to reconfigure the router, you must enter the name of a community with read-write access to the specified router.

On any router that is not configured with a valid SNMP community, Site Manager configures a "public" community with a wildcard manager (using an IP address of 0.0.0.0). This ensures that Site Manager can access the router. You should reconfigure the "public" community, with universal access limited to read-only privileges. For more information, refer to *Configuring SNMP, RMON, BootP, DHCP, and RARP Services*.

MIB Object ID: None

Parameter: Timeout (seconds)

Default: 5

Options: 1 to 300 seconds

Function: Specifies the number of seconds Site Manager waits for a response from the router after it issues an SNMP SET or GET before reissuing the command.

Instructions: Use the slide bar to select the number of seconds for this parameter.

MIB Object ID: None

Parameter: Retries (per request)

Default: 3

Options: 1 to 32 attempts

Function: Specifies the number of times Site Manager will reissue a command when the router does not respond.

Instructions: Use the slide bar to specify the number of retries.

MIB Object ID: None

System Information Parameters

This section describes the parameters in the Edit System Description window.

Parameter:	**System Name**
Default:	None
Options:	Any name
Function:	Identifies this router.
Instructions:	Enter a name for this router.
MIB Object ID:	1.3.6.1.4.1.18.3.3.1.5

Parameter:	**System Contact**
Default:	None
Options:	Any person’s name
Function:	Provides the name of the person to contact about this router.
Instructions:	Enter the name of the contact person, and a way to contact that person.
MIB Object ID:	1.3.6.1.4.1.18.3.3.1.4

Parameter:	**System Location**
Default:	None
Options:	Any place
Function:	Identifies the physical location of this router.
Instructions:	Enter a location description for this router.
MIB Object ID:	1.3.6.1.4.1.18.3.3.1.6

Console Port Parameters

This section describes the parameters in the Console Lists window.

Parameter: **Enable**

Default: Enable (first port)
Disable (other ports)

Options: Enable | Disable

Function: Enables or disables the serial port. The first port on a router is enabled by default. The other ports on routers with multiple serial ports are disabled by default.

Instructions: Select the status of the serial port.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.2

Parameter: **Port Type**

Default: TI

Options: TI

Function: Configures the port for the Technician Interface.

Instructions: Accept the default value.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.7

Parameter: **Baud Rate**

Default: 9600

Options: 9600 | 4800 | 2400 | 1200 | 600 | 300

Function: Specifies the rate of data transfer between the console and the router.

Instructions: Set according to your console requirements.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.8

Parameter: Port Data Bits

Default: 8

Options: 7 | 8

Function: Specifies the number of bits in each ASCII character received or transmitted by the router.

Instructions: Set according to your console requirements.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.9

Parameter: Port Parity

Default: None

Options: None | Odd | Even

Function: Enables or disables data error detection for each character transmitted or received.

Instructions: Set according to your console requirements. Odd or Even enables data error detection. None disables data error detection.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.10

Parameter: Stop Bits

Default: 1

Options: 1 | 1.5 | 2 bits

Function: Specifies the number of bits that follow each ASCII character received or transmitted by the router.

Instructions: Set according to your console requirements.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.11

Parameter: **Enable Modem**

Default: Disable

Options: Enable | Disable

Function: Specifies whether the terminal is connected directly or via a modem to the Technician Interface.

Instructions: Select Enable if the terminal is connected via a modem to the Technician Interface.

Select Disable if the terminal is connected directly to the Technician Interface.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.12

Parameter: **Lines Per Screen**

Default: 24

Options: 1 to 99

Function: Specifies the maximum number of lines displayed on the console screen.

Instructions: Set according to your console requirements.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.13

Parameter: **More Enable**

Default: Enable

Options: Enable | Disable

Function: Specifies whether the Technician Interface pauses after the screen fills with data.

Instructions: Select Enable to configure the Technician Interface to pause after the screen fills with data.

Select Disable to configure the Technician Interface not to pause after the screen fills with data.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.14

Parameter: Prompt

Default: $

Options: Any string of up to 19 keyboard characters other than control key sequences

Function: Specifies the text used as a prompt on your console screen. Place quotation marks around any spaces you want to include in the text string.

Instructions: Accept the default or enter a different text string.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.15

Parameter: Login Timeout

Default: 1

Options: 1 to 99 (99 indicates infinity)

Function: Specifies the number of minutes the Technician Interface waits before timing out when no one presses the Enter key after the `Login:` prompt. This parameter is valid only when Modem Enable is set to Enable. The Technician Interface ends the connection when the timeout value is exceeded.

Instructions: Accept the default, or enter a new timeout value.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.16

Parameter: Password Timeout

Default: 1

Options: 1 to 99 (99 indicates infinity)

Function: Specifies the number of minutes the Technician Interface waits before timing out when no one presses the Enter key after the `Password:` prompt. This parameter is valid only when Modem Enable is set to Enable. The Technician Interface returns to the `Login:` prompt when the timeout value is exceeded.

Instructions: Accept the default, or enter a new timeout value.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.17

Parameter: **Command Timeout**

Default: 15

Options: 1 to 99 (99 indicates infinity)

Function: Specifies the number of minutes that can elapse before the Technician Interface disconnects the session if you do not enter a command at the command prompt. This parameter is valid only when Modem Enable is set to Enable.

Instructions: Accept the default, or enter a new timeout value.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.18

Parameter: **Login Retries**

Default: 3

Options: 1 to 99 (99 indicates infinity)

Function: Specifies the maximum number of login attempts you can make before the Technician Interface disconnects the session. This parameter is valid only when Modem Enable is set to Enable.

Instructions: Accept the default, or enter a new retry value.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.19

Parameter: **Manager Auto Script**

Default: None

Options: Any text string

Function: Specifies the manager’s login script file, which is automatically executed for each login.

Instructions: Enter the name of the login script file for the manager. For more information, refer to *Using Technician Interface Software*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.29

Parameter: **User Auto Script**

Default: None

Options: Any text string

Function: Specifies the user’s login script file, which is automatically executed for each login.

Instructions: Enter the name of the login script file for the user. For more information, refer to *Using Technician Interface Software*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.30

Parameter: **Force User Logout Enable**

Default: Disable

Options: Enable | Disable

Function: Enabling this option forces the user to log out if he or she tries to escape from the autoscript.

Instructions: Select Enable to force the user to log out if an attempt is made to escape the autoscript.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.11.1.1.31

RUI Boot Group List Parameter

This section describes the parameter in the RUI Boot Group List window.

Parameter: Enable

Default: Enable

Options: Enable | Disable

Function: Enables or disables a scheduled boot for a group of routers that you designate.

Instructions: Select Disable to prevent routers from booting according to the schedule you defined. Otherwise, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.1.2

RUI Boot Interface Parameters

This section describes the parameters in the RUI Boot Interface Parameters window.

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables a scheduled boot of a particular router.

Instructions: Select Disable to prevent a scheduled boot of a particular router. Otherwise, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.2

Parameter: **Image Name**

Default: None

Options: Any valid boot image file, for example, *bn.exe*, along with the volume that contains this file

Function: Designates which image file the router uses to boot.

Instructions: Enter the volume and image file name in the format <*volume*>:<*image file*>, for example *2:bn.exe*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.5

Parameter: **Configuration File Name**

Default: None

Options: Any valid configuration file, along with the volume that contains the configuration file

Function: Designates the configuration file that the router uses to boot.

Instructions: Enter the volume and configuration file name in the format <*volume*>:<*configuration file*>, for example *2:config*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.6

RUI Boot Parameters

This section describes the parameters in the RUI Boot Parameters window.

Parameter:	**Year**
Default:	None
Options:	1970 to 2070
Function:	Specifies the year that the scheduled boot will occur.
Instructions:	Specify a year.
MIB Object ID:	None

Parameter:	**Month**
Default:	None
Options:	1 to 12
Function:	Specifies the month of the year that the scheduled boot will occur.
Instructions:	Enter an integer for a specific month.
MIB Object ID:	None

Parameter:	**Day**
Default:	None
Options:	1 to 31
Function:	Specifies the date of the month that the scheduled boot will occur.
Instructions:	Enter an integer for the day of the month.
MIB Object ID:	None

Parameter: **Hour**

Default: None

Options: 0 to 23

Function: Specifies the hour of the day that the scheduled boot will occur.

Instructions: Enter an integer from 0 to 23 for the hour.

MIB Object ID: None

Parameter: **Minute**

Default: None

Options: 0 to 59

Function: Specifies the minute of the hour that the scheduled will occur.

Instructions: Enter an integer from 0 to 59 for the minute.

MIB Object ID: None

Parameter: **Second**

Default: None

Options: 0 to 60

Function: Specifies the second that the scheduled boot will occur.

Instructions: Enter an integer from 0 to 60 for the second.

MIB Object ID: None

Parameter: **Boot Image Name**

Default: None

Options: Any valid boot image file, for example, *bn.exe*, along with the volume that contains this file

Function: Specifies which image file the router uses to boot.

Instructions: Enter the volume and image file name in the format <*volume*>:<*image file*>, for example, *2:bn.exe*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.5

Parameter: **Boot Configuration File**

Default: None

Options: Any valid configuration file, along with the volume that contains the configuration file

Function: Specifies the configuration file that the router uses to boot.

Instructions: Enter the volume and configuration file name in the format <*volume*>:<*configuration file*>, for example, *2:config*.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.6

Parameter: **Local Time/UTC Offset**

Default: None

Options: LOCAL | PLUS | MINUS

Function: Specifies whether the local time zone is ahead of or behind the Universal Time Code (UTC).

Instructions: Enter PLUS if your time zone is ahead of the Universal Time Code (UTC) or MINUS if it is behind the Universal Time Code (UTC). Enter the value in uppercase letters. Do not enter LOCAL unless the UTC offset of the router’s system clock is set to 0. Refer to Chapter 1 for instructions on setting the router’s time.

After you enter PLUS or MINUS, the Hours from UTC and Minutes from UTC parameters become active.

MIB Object ID: None

Parameter: **Hours from UTC**

Default: None

Options: 0 to 11

Function: Specifies the number of hours that the local time zone differs from the Universal Time Code (UTC).

Instructions: Enter an integer that reflects the difference in hours between the local time zone and the UTC.

MIB Object ID: None

Parameter: **Minutes from UTC**

Default: None

Options: 0 to 59

Function: Specifies the number of minutes that the local time zone differs from the Universal Time Code (UTC).

Instructions: Enter an integer that reflects the difference in minutes between the local time zone and the UTC.

MIB Object ID: None

Trap Parameters

This section describes the parameters in the Trap Port and Trap Types window.

Parameter: **Trap Port**

Default: 162

Options: 1 to 9999

Function: Specifies the number of the port on the Site Manager workstation to which the SNMP agent sends traps.

Instructions: Accept the default, 162, or change the UDP port number to use a different port for the Site Manager workstation. Do not use a port used by another application.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.1.5

Parameter: **Trap Types**

Default: Generic

Options: All | Generic | Specific | None

Function: Specifies the type of trap messages that are sent to the SNMP manager.

Instructions: Select the types of traps that you want to receive. Refer to Chapter 7 for an explanation of each trap type.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.1.6

Ping Parameters

This section describes the parameters in the Ping at Intervals window.

Parameter: **IP Address**

Default: None

Options: 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

Options: Any name you want for the device from which you are trying to connect.

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

Options: 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 | 15 (APPN only)

Options: 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.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.6

Parameter: **Ping Retry**

Default: 0

Options: 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

Options: 1 to 65535

Function: Specifies the amount of time (in milliseconds) to wait before sending the next ICMP echo packet.

Instructions: Enter a value from 1 to 65535.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.9

Parameter: **Timer**

Default: 0

Options: Any integer

Function: Specifies the number of minutes that will pass before the ping occurs again.

Instructions: Enter an integer, 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

Options: PING_NOTRACE | PING_TRACE

Function: Lets you turn on the Trace Routes feature 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, accept 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

Options: 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 terminates.

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 Source Route to specify the routes.

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

Options: 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. This should be the IP address of the outgoing port on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.13

Parameter: **Ping Type of Service**

Default: NORMAL

Options: NORMAL | PRIORITY | IMMEDIATE | FLASH | FLASH_OVERRIDE | CRITIC_ECP | INTERNETWORK_CONTROL | NETWORK_CONTROL

Function: Specifies the quality of service (service precedence) for handling the ICMP packet.

Instructions: Accept the default, NORMAL, for routine service, or choose one of the other types of service. Refer to an IP programmer's manual for information about 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

Options: 1 to 60

Function: If the ping is on a timer (that is, if you set the Timer parameter to a value other than 0), 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 to 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

Syslog Group Parameters

This section describes the parameter in the Syslog Group Parameters window.

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the syslog facility on the router.

Instructions: Set to Disable if you want to disable the syslog facility on the router. Note that even though the syslog facility is enabled by default, you must use Site Manager to configure a remote host and enable associated filters before the syslog facility can filter and forward messages.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.1.2

Syslog Host List Parameters

This section describes the parameters in the Syslog Host List window.

Parameter: **Messaging Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the forwarding of router events to this remote host.

Instructions: If you want syslog to forward router events to this host, accept the default. Otherwise, choose Disable.

You can also stop the forwarding of router events to the host by deleting the host. If you delete a remote host and later decide you want to forward router events to that host, you must add the remote host again.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.2.1.2

Parameter: **Host UDP Port**

Default: 514

Options: 514 to 530

Function: Identifies the UDP port of the remote host.

Instructions: Type the port number to which you want syslog to send UDP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.2.1.4

Parameter: Host Log Facility

Default: LOCAL7

Options: LOCAL0 to LOCAL7

Function: Specifies the facility type that syslog appends to router event messages as part of the priority code. The syslogd daemon on the remote host uses this information to determine which system generated the message that syslog forwarded.

Instructions: Specify the facility type you want to use. You must also specify the facility type in the *syslog.conf* file on the remote host so that the syslogd daemon knows where to direct event messages from this facility.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.2.1.5

Parameter: Host Time Seq Enable

Default: Disable

Options: Enable | Disable

Function: Forwards to the remote host router event messages in the order that they occur.

Instructions: Enable this feature only if it is essential that the remote host receive router event messages in the order that they occur.

When this feature is enabled, the syslog facility polls the router, filters the event messages, orders them based on the time they occurred, and then forwards them to the remote hosts.

When this feature is disabled, the syslog facility polls the router, filters the event messages, and then forwards the messages to the remote hosts.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.2.1.6

Parameter: **Maximum Hosts**

Default: 5

Options: 1 to 10

Function: Specifies the maximum number of remote hosts you want to configure for the syslog facility.

Instructions: Type the maximum number of hosts that will use the syslog facility.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.1.4

Parameter: **Log Poll Timer**

Default: 5

Options: 5 to 610,000 seconds

Function: Specifies the amount of time (in seconds) that syslog waits before initiating another cycle to poll all slots for event messages the router logged since the previous polling cycle.

Instructions: Type the number of seconds that syslog waits between polling cycles.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.1.5

Syslog Host Filter List Parameters

This section describes the parameters in the Syslog Host Filter List window.

Parameter: **Filter Entity Name**

Default: None

Options: Any valid entity name

Function: Specifies the entity whose log messages you want to forward to the remote host.

Instructions: Type the name of the entity whose log messages you want to forward to the remote host. You can click on Values and select an entity name from the list that appears. Also, *Event Messages for Routers* provides a complete list of entity names.

If you select the entity name WILDCARD, syslog uses the parameters that you specify for this filter only if no other operational filters exist for the remote host. In such cases, syslog applies the filters of the wildcard entity to all event messages regardless of the entity.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.4

Parameter: **Filter Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the filter for the associated remote host.

Instructions: If you want the syslog facility to use this filter to determine which messages to forward to the remote host, choose Enable. Otherwise, choose Disable.

You can stop using this entity filter by deleting the filter. To do this, select the filter in the Syslog Host Filter List window, and then click on Delete. If you delete an entity filter and later decide you want to use that filter, you must add the filter again.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.2

Parameter: **Log Evt Lower Bound**

Default: 0

Options: 0 to 255

Function: Along with the Log Evt Upper Bound parameter, specifies the event number (code) or range of event numbers (for the current filter) that you want to forward to the remote host

Instructions: To specify a range of event numbers that you want to use in the filter, type the lower number of the range in this field. You then type the upper number of the range in the Log Evt Upper Bound parameter.

The values you type for lower and upper bound are included in the range. For example, if you specify a lower bound of 2 and an upper bound of 7, syslog forwards all messages that are of event codes 2 through 7, inclusive. The syslog facility ignores all other event messages.

To filter a specific event code, type the event code in this parameter. Be sure to type the same code in the Log Evt Upper Bound parameter. For example, to forward only the log messages that have an event code of 10, type 10 in this field and in the Log Evt Upper Bound parameter.

If you do not want to filter by event code, accept the default, 0. Be sure to accept the default in the Log Evt Upper Bound parameter.

If you use the wildcard filter entry, 255, the syslog facility ignores this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.7

Parameter: **Log Evt Upper Bound**

Default: 255

Options: 0 to 255

Function: Along with the Log Evt Lower Bound parameter, specifies the event number (code) or range of event numbers (for the current filter) that you want to forward to the remote host

Instructions: To specify a range of event numbers, type the upper number of the range in this field. You must specify the lower number of the range in the Log Evt Lower Bound parameter.

The values you type for lower and upper bound are included in the range. For example, if you specify a lower bound of 2 and an upper bound of 7, syslog forwards all messages that are of event codes 2 through 7, inclusive. The syslog facility ignores all other event messages.

To filter a specific event code, type the event code in this parameter. You must type the same event code in the Log Evt Lower Bound parameter. For example, to forward only the log messages that have an event code of 10, type 10 in this field and in the Log Evt Lower Bound parameter.

If you do not want to filter by event code, accept the default, 255. Be sure to accept the default in the Log Evt Lower Bound parameter.

If you use the wildcard filter entry, 255, the syslog facility ignores this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.8

Parameter: **Severity Mask**

Default: None

Options: w | i | t | f | d

Function: Identifies the types of event severity to forward.

Instructions: If you specified a range of event numbers (using the Log Evt Lower Bound and Log Evt Upper Bound parameters), syslog ignores this parameter.

If you did not specify a range of event numbers, enter the types of events you want to forward. The syslog facility ignores any events that you do not specify. Use the first letter of each severity type you want to include:

w - warning

i - informational

t - trace

f - fault

d - debug

Be sure to type lowercase letters only. Do not separate the letters with commas or spaces.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.9

Parameter:	**Slot Lower Bound**
Default:	0
Options:	0 to 14
Function:	Along with the Slot Upper Bound parameter, specifies the slot or range of slots on which you want to filter the log messages for this entity. (In the case of ASN routers, this parameter specifies the module for the particular slot because an ASN router is considered a slot.)
Instructions:	To specify a range of slots, type the lower number of the range in this parameter. You then type the upper number of the range in the Slot Upper Bound parameter. The values you type for lower and upper bound are included in the range. For example, if you specify a lower bound of 1 and an upper bound of 4, syslog forwards all messages that occur on slots 1 through 4, inclusive. The syslog facility ignores event messages that occur on all other slots. To filter events for a specific slot, type the slot number in this field. Be sure to type the same number in the Slot Upper Bound field. For example, to forward only the log messages that occur on slot 2, type 2 in this parameter and in the Slot Upper Bound parameter. If you do not want to use this filter, accept the default, 0. Be sure to accept the default in the Slot Upper Bound parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.10

Parameter: **Slot Upper Bound**

Default: 0

Options: 0 to 14

Function: Along with the Slot Lower Bound parameter, specifies the slot or range of slots on which you want to filter the log messages for this entity. (In the case of ASN routers, this parameter specifies the module for the particular slot because an ASN router is considered a slot.)

Instructions: To specify a range of slots, type the upper number of the range in this parameter. You must specify the lower number of the range in the Slot Lower Bound parameter.

The values you type for lower and upper bound are included in the range. For example, if you specify a lower bound of 1 and an upper bound of 4, syslog forwards all messages that occur on slots 1 through 4, inclusive. The syslog facility ignores event messages that occur on all other slots.

To filter events for a specific slot, type the slot number in this parameter. You must type the same number in the Slot Lower Bound parameter. For example, to forward only the log messages that occur on slot 2, type 2 in this parameter and in the Slot Lower Bound parameter.

If you do not want to use this filter, accept the default, 0. Be sure to accept the default in the Slot Lower Bound parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.11

Parameter: **Fault Map**

Default: CRIT

Options: EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG

Function: Maps router event messages with a severity level of fault to an error level that the UNIX syslogd daemon recognizes. Table B-1 describes each of these error levels.

Instructions: Bay Networks recommends that you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then choose the error level you want.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.12

Table B-1. syslogd Error Levels

Error Level	Description
EMERG	A panic condition that the syslogd daemon normally broadcasts to all users
ALERT	A condition, such as a corrupted system database, that you should correct immediately
CRIT	Critical conditions, such as hard device errors
ERR	Errors
WARNING	Warning messages
NOTICE	Conditions that are not errors, but may require special handling
INFO	Informational messages
DEBUG	Messages that contain information that is of value only when you are debugging the network

Parameter: Warning Map

Default: WARNING

Options: EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG

Function: Maps router event messages with a severity level of warning to an error level that the UNIX syslogd daemon recognizes. See Table B-1 for a description of the syslogd error levels.

Instructions: Bay Networks recommends that you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then choose the error level you want.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.13

Parameter: **Info Map**

Default: INFO

Options: EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG

Function: Maps router event messages with a severity level of info to an error level that the UNIX syslogd daemon recognizes. See Table B-1 on page B-32 for a description of the syslogd error levels.

Instructions: Bay Networks recommends that you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then choose the error level you want.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.14

Parameter: **Trace Map**

Default: DEBUG

Options: EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG

Function: Maps router event messages with a severity level of trace to an error level that the UNIX syslogd daemon recognizes. See Table B-1 on page B-32 for a description of the syslogd error levels.

Instructions: Bay Networks recommends that you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then choose the error level you want.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.15

Parameter:	**Debug Map**
Default:	DEBUG
Options:	EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG
Function:	Maps router event messages with a severity level of debug to an error level that the UNIX syslogd daemon recognizes. See Table B-1 on page B-32 for a description of the syslogd error levels.
Instructions:	Bay Networks recommends that you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then choose the error level you want.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.16

Appendix C
Checking SNMP SET Errors

Occasionally, you may receive an SNMP SET error when you try to connect to a router in dynamic mode. SET errors lock you out of the router for a period of time (the default lockout time is 2 minutes). The router displays one of the following SET error messages:

- `SNMP General Set Error! Machine is currently locked by Manager (IP Address)`
- `SNMP set error`

The SNMP General Set Error message appears when an SNMP SET lockout condition exists on a the target router.

Common causes for these errors include the following:

- Another person is connected to the router you are attempting to configure.
- An SNMP request from your Site Manager workstation timed out due to traffic conditions on the network.
- The SNMP community name that you specified for the SNMP request did not allow write access to the desired router.

When you are locked out of the router, it may mean that the router rejected one or more of your SET attempts, or you may need to modify part of your configuration.

For more information about router SNMP SET errors, refer to *Configuring SNMP, RMON, BootP, DHCP, and RARP Services*.

Receiving an SNMP SET Error

When you receive an SNMP SET error message, click on OK in the error message box and see if another SET error message appears. If no other SET error message appears immediately, try the SET operation again.

If several SET error messages appear in succession while you are in dynamic mode, wait for the router's SNMP lockout condition to clear, then follow these steps:

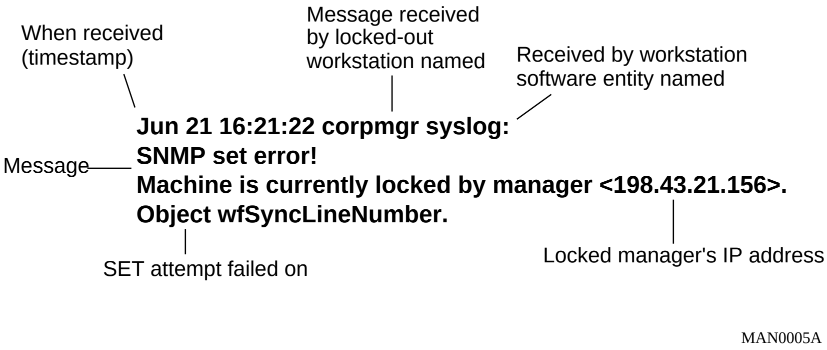
1. **Delete the circuit you are attempting to configure.**
2. **Add the circuit again.**
3. **Repeat the rest of your configuration.**

If the previous steps fail:

1. **Exit the Configuration Manager without saving your changes.**
2. **Reboot the router with the current (last saved) configuration file.**
3. **Re-create your entire configuration.**

Accessing the SNMP SET Error Log

Your Site Manager workstation can log SNMP SET errors that the router receives. Figure C-1 shows the logged version of the SET lockout error message.



```
Jun 21 16:21:22 corpmgr syslog:
SNMP set error!
Machine is currently locked by manager <198.43.21.156>.
Object wfSyncLineNumber.
```

Figure C-1. Logged Version of SNMP SET Error Message

By logging the errors, you can examine them and discover their cause. You can examine the default or designated SNMP SET error log file on your Site Manager workstation.

The following sections explain how to specify a destination for the SNMP SET errors on a UNIX workstation or a PC.

Error Messages on a UNIX Workstation

UNIX Site Manager workstations use the standard UNIX syslog facility and *syslog.conf* file to specify destinations for SNMP SET error messages. Refer to the instructions provided in the UNIX man pages for information on syslog and *syslog.conf*.

To determine the current destination for the error messages, check the facility level, *user.err*, in the */etc/syslog.conf* file. The path next to each user.err entry indicates a destination for SNMP SET error messages.

Modify the *syslog.conf* file if you want to change the destination for SNMP SET error messages.

Error Messages on a PC

On a PC, the destination for the SNMP SET error messages is listed in the *seterror.log* file (*C: \wf \seterror.log*).

Appendix D
Configuring the syslog Facility

Bay Networks provides an implementation *syslog* facility that works with the UNIX *syslogd* daemon residing on remote host systems. The syslog facility periodically polls the router's event log and forwards any new router event messages to the remote hosts that you specify. The UNIX syslogd daemon then sends the messages to the appropriate device.

If you use Site Manager, you can use the Events Manager to examine router events. However, if you manage your routers using a third-party SNMP-based network management application, such as the Hewlett-Packard OpenView Network Node Manager, you can use the syslog facility as an alternative to SNMP traps for displaying router events.

To configure the syslog facility, you use the Configuration Manager. The Configuration Manager does the following:

- Delivers event messages in the order in which they occur
- Filters messages based on a set of criteria that you define
- Enables or disables the syslog facility

This appendix contains the following information:

Configuring the syslogd Daemon

You must configure the UNIX syslogd daemon to specify the log files and the remote hosts that should receive event messages. To do this, you must edit the file *etc/syslog.conf* on each remote host.

The syslogd daemon determines where to write event messages based on the following:

- A *priority code* that the syslog application attaches to each event message
- Event data from the *syslog.conf* file

The priority code consists of a *facility* and a *level*.

- The *facility* describes the system that originates the event message using the standard (configurable) UNIX facility names LOCAL0 through LOCAL7.
- The *level* is the UNIX error level (emerg, alert, crit, err, warning, notice, info, debug) that you associate with the event message severity level (fault, trace, warning, information, and debug).

For example, you might map all router fault messages to the UNIX CRIT error level. You can map more than one router severity level to the same UNIX error level.

You can also assign a facility and severity levels to error levels. For example, suppose you want to log all fault, warning, and debug messages that the syslogd daemon receives from the router to a file, for example, */usr/adm/logs/baynet.log*, on the remote host. Assume also that you used Site Manager to map fault messages to the CRIT error level, warning messages to the WARNING error level, and debug messages to the UNIX DEBUG level.

You might add a line similar to the following to your *syslog.conf* file:

```
local7.crit;local7.warning;local7.debug /usr/adm/logs/baynet.log
```

Be sure that you use a tab before the path to the file, in this example, */usr/adm/logs/baynet.log*.

In this example, the facility is LOCAL7.

For more information about the syslogd daemon and the *syslog.conf* file, refer to the instructions provided in the UNIX man pages.

Understanding How syslog Filters Messages

The syslog facility forwards router event messages to a remote host only if there is an *entity filter* for that host. An entity filter is a set of criteria that you specify to tell syslog whether to forward an event message. Entities include Bay Networks software that provides a service, such as TFTP, IP, or the GAME operating system.

Refer to *Event Messages for Routers* for a complete list of entities for which you can create filters.

You can define many entity filters for a remote host, and you can define different criteria for each entity. For example, you might define two different APPN filters for the same host.

The entity filter can filter messages based on the following criteria:

- The event number or range of numbers

  For example, you might want syslog to forward only the event messages with event numbers 5 through 50.

- The severity level (warning, fault, trace, information, or debug)
- The slot or range of slots on which the event occurred

  For example, you might want only the event messages that occur on slot 4, or on slots 2 through 4.

➡ **Note:** You can filter events by either event number or event severity level, but not by both.

Configuring the syslog Facility

To configure the syslog facility on the router:

1. **Configure the syslog group parameters.**

   The group parameters let you

   - Enable or disable syslog on the router.
   - Specify the number of remote hosts you want to configure for syslog.
   - Set the polling cycle.

2. **Configure a list of hosts that should receive router event messages.**

The following sections describe how to access syslog parameters and enable the syslog facility.

Configuring syslog Group Parameters

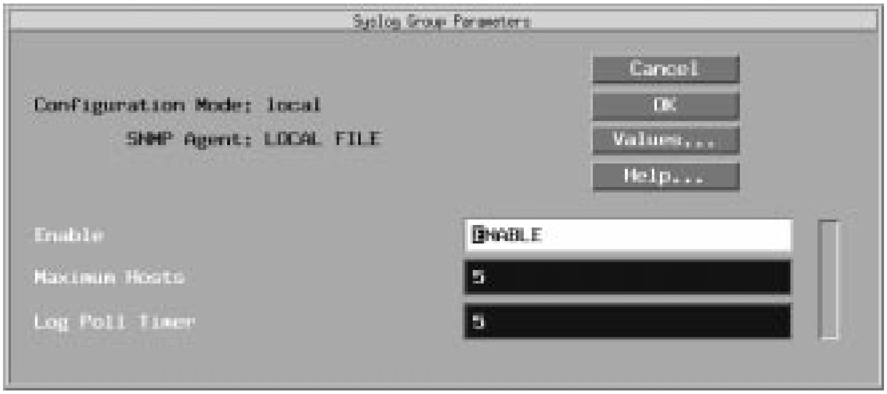
To configure the syslog group parameters:

1. **In the main Site Manager window, choose Tools > Configuration Manager.**

   The Configuration Manager window opens.

2. **Choose Platform > Syslog > Create Syslog.**

   The Syslog Group Parameters window opens (Figure D-1).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Enable ENABLE
Maximum Hosts 5
Log Poll Timer 5

Figure D-1. Syslog Group Parameters Window

3. **Enter values for the parameters.**

   Refer to the parameter descriptions beginning on page B-22 or click on Help.

4. **Click on OK.**

   You return to the Configuration Manager window.

   After you enable syslog, you can edit the syslog group parameters at any time by choosing Platform > Syslog > Global in the Configuration Manager window.

Configuring the syslog Host List

To specify which remote hosts receive router event messages, add them to the syslog host list.

To configure the syslog host list:

1. **In the main Site Manager window, choose Tools > Configuration Manager.**
2. **Choose Platform > Syslog > Syslog Host Table.**

   The Syslog Host List window opens (Figure D-2).

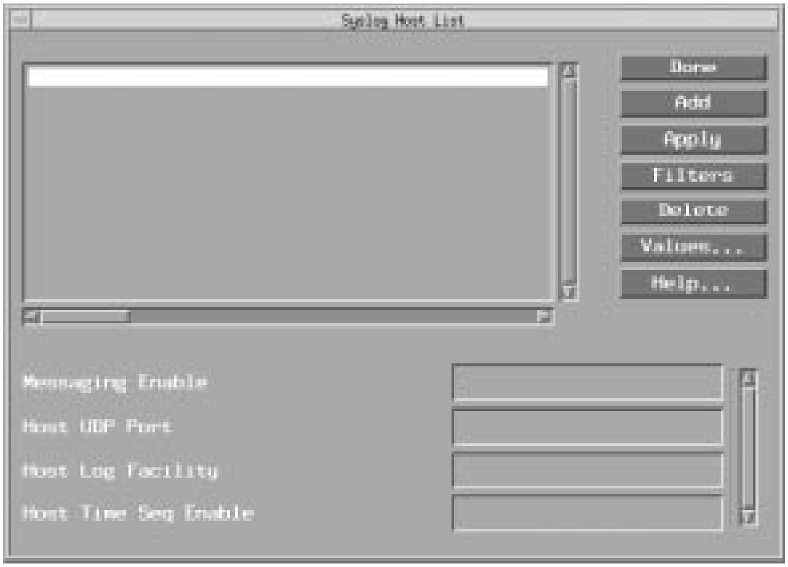
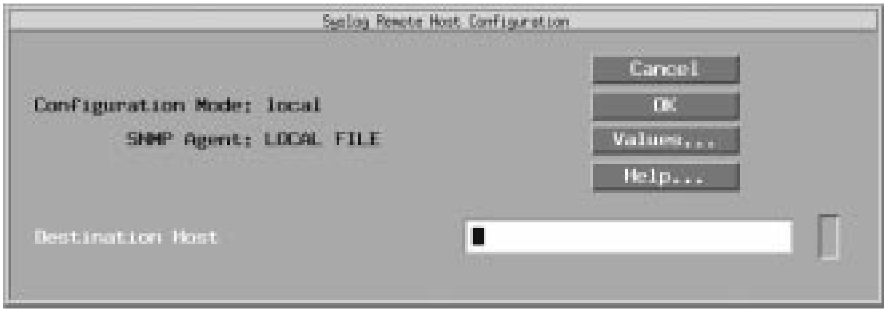


Figure D-2. Syslog Host List Window

3. **Click on Add.**

   The Syslog Remote Host Configuration window opens (Figure D-3).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Figure D-3. Syslog Remote Host Configuration Window

4. **Type the IP address of the host, then click on OK.**

   The Syslog Host Filter List window opens (Figure D-4).

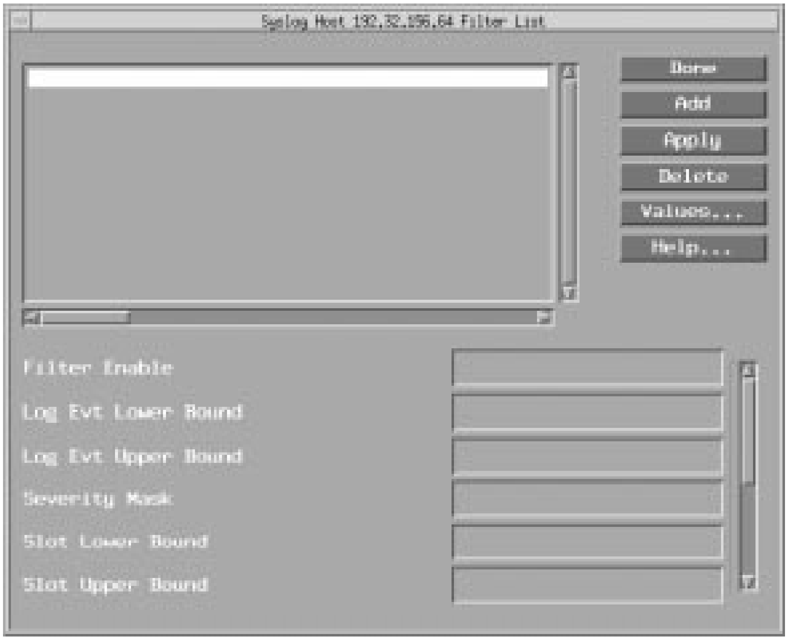
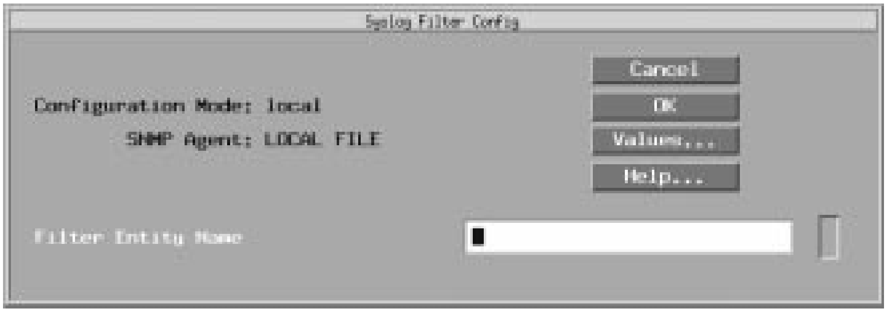


Figure D-4. Syslog Host Filter List Window

5. **Click on Add.**

   The Syslog Filter Config window opens (Figure D-5).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Filter Entity Name

Figure D-5. Syslog Filter Config Window

6. **Type the Filter Entity Name, then click on OK.**

   You return to the Syslog Host Filter List window (refer to Figure D-4).

   The IP address of the host, the filter number, and the filter index appear in the list.

7. **Define the filter by entering values for the filter parameters.**

   Refer to the parameter descriptions beginning on page B-26 or click on Help.

8. **Click on Apply.**

9. **To add more filters, repeat steps 5 through 8.**

10. **Click on Done.**

Deleting the syslog Facility from the Router

To delete the syslog facility from the router:

1. **Open the Configuration Manager window.**
2. **Choose Platform > Syslog > Delete Syslog.**

   A window prompts you to confirm your decision:

   ```
   Do you REALLY want to delete Router Syslog?
   ```
3. **Click on OK in the confirmation window.**

Appendix E
Reallocating Memory Partitions for a Processor Module

Using the Site Manager's Kernel Configuration tool, you can reallocate global and local 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.
- ANH -- The ANH router contains a single processor module.
- ASN -- The ASN router contains a single processor module.
- ACE-32 (8 MB or greater) -- The ACE-32 processor module is used in VME-based routers: CN, LN, FN, and ALN.
- FRE-2 -- The FRE-2 processor module is used in the BLN, BLN-2, and BCN routers.

Partitioning Overview

Router processor modules use three types of memory:

- Global
- Local
- 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.

Table E-1 describes how NVRAM supports the processor modules in PPX-bus and VME-bus routers.

Table E-1. NVRAM Storage for PPX-Based and VME-Based Routers

Module	NVRAM Storage
FRE-2 (PPX-based routers)	NVRAM is present on each FRE-2 processor module inside the router. If you move a FRE-2 module to another slot in the router, the memory partitioning configuration moves with the FRE-2 module to the new slot.
ACE-32 (VME-based routers)	NVRAM is present only on the SYSCON processor module. If you move an ACE-32 module to another slot in the router, the memory partitioning configuration does not move with the ACE-32 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 module.

Site Manager does not let you allocate more than 4 MB of global memory to an ACE-32 processor module if an ACE-25 module resides in the same router. You can overcome this constraint by upgrading any ACE-25 processors in the same router to ACE-32 processors.

Repartitioning Global and Local Memory

Caution: Change memory partitioning only at the recommendation of, or under the direction of, the Bay Networks Technical Solutions Center. Under normal router and network operating conditions, there is 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.

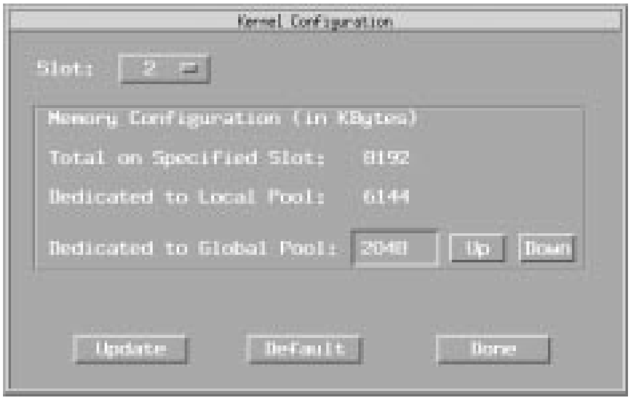
To repartition global and local memory:

1. **Connect to the router.**

   Refer to Chapter 1 for instructions.

2. **In the main Site Manager window, choose Administration > Kernel Configuration.**

   The Kernel Configuration window opens (Figure E-1).



Kernel Configuration

Slot: 2

Memory Configuration (in KBytes)

Total on Specified Slot: 8192

Dedicated to Local Pool: 6144

Dedicated to Global Pool: 2048

Figure E-1. Kernel Configuration Window

If the router you are configuring is not an AN, ANH, AFN, or ASN, or if the router does not contain an ACE-32 or a FRE-2 processor module, a window opens 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, for example, when the Kernel Configuration routine finds only ACE-25 or FRE modules in the currently connected router.

The Kernel Configuration window displays the following information (Table E-2).

Table E-2. Kernel Configuration Window Information

Memory Configuration Information	Description
Total memory on the specified slot	Total memory displayed depends on the type of processor module.
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 learned.
Memory dedicated to the global pool	Global pool refers to the memory dedicated for message buffers.

3. **Select the processor module slot that requires memory repartitioning.**
4. **Enter an amount in the Dedicated to Global Pool field.**

   To add more memory to the global pool, click on Up 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 Down until the desired amount of memory appears, or type a value in the field.
5. **Click on Update to restart the slot with the new values.**

   A confirmation window prompts:

   ```
   Restart slot?
   ```

   To reset the memory allocation to the factory-default values, click on Default instead of Update. A message then prompts you to confirm your decision to reset the values.
6. **Click on OK to restart the processor module located in that slot.**

   You return to the main Site Manager window.

Site Manager stores the new configuration in NVRAM and restarts the module (ACE-32 or FRE-2) or router (AN, ANH, AFN, or ASN). This store-and-restart process takes about 10 seconds to complete.

7. **Repeat steps 2 through 6 to reallocate memory partitioning on a different processor module, if applicable.**

   Repeat steps 1 through 6 to reallocate memory partitioning for a module in a different router.

8. **Click on Done.**

Index