IRM2 User's Guide

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Enterasys Networks makes no representations or warranties to the effect that the Licensed Software is virus-free.

Printed in the United States of America.

Order Number: 9031597-04 April 2000

Enterasys Networks
P.O. Box 5005
Rochester, NH 03866-5005

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

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

   Enterasys Networks, 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.

   (b) This computer software may be:

   (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;

   (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

   (3) Reproduced for safekeeping (archives) or backup purposes;

   (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;

   (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and

   (6) Used or copied for use in or transferred to a replacement computer.

   (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

   (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

   (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Contents

Chapter 1 Introduction

Chapter 2 The IRM2 Chassis View

Chapter 3 Statistics

Chapter 4 Source Address Functions

Chapter 5 Alarm Limits

Chapter 6 Trap Selection

Chapter 7 Redundancy

Chapter 8 Redundancy (Continued)

Index

Chapter 1

Introduction

How to use this guide; related guides; software conventions; getting help; IRM2 firmware versions

Welcome to the Enterasys Systems ***NetSight Element Manager for the IRM2 User's Guide.*** We have designed this guide to serve as a simple reference for using NetSight Element Manager for the IRM2.

The IRM2 is an IEEE 802.3-compliant repeater module designed to be installed in a Cabletron Systems Multi Media Access Center (MMAC®) hub, either with or without the Flexible Network Bus (FNB™). The IRM2 occupies the first (management) slot of the MMAC hub, and controls non-intelligent Ethernet modules installed to its left. It retimes and regenerates Ethernet data packets throughout the chassis, and performs automated management such as port segmentation. With NetSight Element Manager, you can gather a full array of statistical information from the IRM2 at the device, board, and port levels — including data throughput statistics and error breakdowns. You can also set alarms and traps for the hub, configure redundant circuits, or set port security parameters based on Ethernet source address locking.

Using This Manual

Each chapter in this guide describes one major functionality or a collection of several smaller functionalities of the IRM2 device module. This guide contains information about software functions which are accessed directly from the device icon; for information about functions which are accessed via the menu bar across the top of the map window, consult the ***User's Guide*** and ***Tools Guide*** included in this package, as well as any management platform-specific documentation that accompanied NetSight Element Manager.

Chapter 1, **Introduction**, provides a list of related documentation, describes certain software conventions, and shows you how to contact the Enterasys Global Call Center.

Chapter 2, **The IRM2 Chassis View**, describes the visual display of the IRM2-controlled chassis and explains how to use the mouse within the Chassis View; the operation of several chassis-level management functions — such as changing the chassis display, naming boards, enabling and disabling boards and ports, and setting device date and time — is also described here.

Chapter 3, **Statistics**, describes the Statistics, Timer Statistics, Summary Statistics, and Performance Graph selections available at the repeater, board, and port levels. Each of these selections provides a slightly different view of the network information being collected by your IRM2.

Chapter 4, **Source Address Functions**, describes how to display the Source Address lists, how to set the ageing time, and how to locate the port being used by a specific source address; it also discusses the effects of port locking.

Chapter 5, **Alarm Limits**, provides instructions on setting Alarm Limits for the repeater, or for an individual board or port.

Chapter 6, **Trap Selection**, details how to use the Trap Selection window to determine whether your IRM2 will send certain common SNMP traps to your Enterasys management station.

Chapter 7, **Redundancy**, describes how to configure redundant circuits for your IRM2 repeater, to ensure that vital network connections remain open and active.

We assume that you have a general working knowledge of Ethernet IEEE 802.3- and FDDI-type data communications networks and their physical layer components, and that you are familiar with general bridging concepts.

Related Manuals

The ***IRM2 User's Guide*** is only part of a complete document set designed to provide comprehensive information about the features available to you through NetSight Element Manager. Other guides which include important information related to managing the IRM2 include:

Enterasys' ***NetSight Element Manager User's Guide***

Enterasys' ***NetSight Element Manager Tools Guide***

Enterasys' ***NetSight Element Manager Remote Administration Tools User's Guide***

Enterasys' ***NetSight Element Manager Remote Monitoring (RMON) User's Guide***

Enterasys' ***NetSight Element Manager Alarm and Event Handling User's Guide***

Enterasys' ***Network Troubleshooting Guide***

Microsoft Corporation's ***Microsoft Windows User's Guide***

For more information about the capabilities of the IRM2, consult the appropriate hardware documentation.

Software Conventions

NetSight Element Manager’s user interface contains a number of elements which are common to most windows and which operate the same regardless of which window they appear in. A brief description of some of the most common elements appears below; note that the information provided here is not repeated in the descriptions of specific windows and/or functions.

Using the Mouse

This document assumes you are using a Windows-compatible mouse with two buttons; if you are using a three button mouse, you should ignore the operation of the middle button when following procedures in this document. Procedures within the NetSight Element Manager document set refer to these buttons as follows:

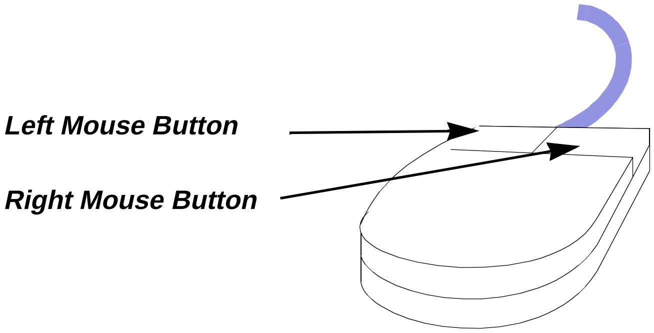


Figure 1-1. Mouse Buttons

For many mouse operations, this document assumes that the left (primary) mouse button is to be used, and references to activating a menu or button will not include instructions about which mouse button to use.

However, in instances in which right (secondary) mouse button functionality is available, instructions will explicitly refer to **right** mouse button usage. Also, in situations where you may be switching between mouse buttons in the same area or window, instructions may also explicitly refer to both **left** and **right** mouse buttons.

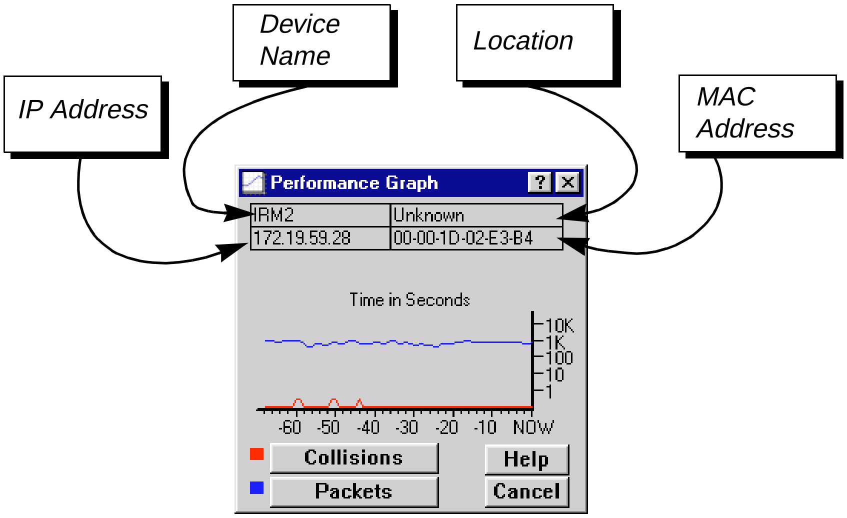
Instructions to perform a mouse operation include the following terms:

- **Pointing** means to position the mouse cursor over an area without pressing either mouse button.
- **Clicking** means to position the mouse pointer over the indicated target, then press and release the appropriate mouse button. This is most commonly used to select or activate objects, such as menus or buttons.

- **Double-clicking** means to position the mouse pointer over the indicated target, then press and release the mouse button two times in rapid succession. This is commonly used to activate an object's default operation, such as opening a window from an icon. Note that there is a distinction made between "click twice" and "double-click," since "click twice" implies a slower motion.
- **Pressing** means to position the mouse pointer over the indicated target, then press and hold the mouse button until the described action is completed. It is often a pre-cursor to Drag operations.
- **Dragging** means to move the mouse pointer across the screen while holding the mouse button down. It is often used for drag-and-drop operations to copy information from one window of the screen into another, and to highlight editable text.

Common IRM2 Window Fields

Similar descriptive information is displayed in boxes at the top of most device-specific windows in NetSight Element Manager, as illustrated in Figure 1-2, below.



IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

Figure 1-2. Sample Window Showing Informational Boxes

Device Name

Displays the user-defined name of the device. The device name can be changed via the System Group window; see the ***Generic SNMP User's Guide*** for details.

IP Address

Displays the device's IP (Internet Protocol) address. This will be the IP address used to define the device icon. IP addresses are assigned via Local Management for the IRM2; they cannot be changed via NetSight Element Manager.

Location

Displays the user-defined location of the device. The location is entered through the System Group window; see the ***Generic SNMP User's Guide*** for details.

MAC Address

Displays the manufacturer-set MAC address of the IRM2 with which NetSight Element Manager is communicating. This address is factory-set and cannot be altered.

Informational fields describing the boards and/or ports being modeled are also displayed in most windows:

Board Number

Displays the number indicating the position of the monitored board in the chassis.

Board Name

Displays the user-entered name for the board. You can change the board name via the **Name** option available from the Board menu.

Port Number

Displays the number of the monitored port.

Port Name

Displays the user-defined name of the port. You can change the port name via the **Name** option available from the Port menu.

Active Users

Indicates the number of users processing information through the IRM2 repeater, board, or port, as determined by MAC addresses.

Uptime

Displays the amount of time, in a days hh:mm:ss format, that the IRM2 has been running since the last start-up.

Using Window Buttons

The Cancel button that appears at the bottom of most windows allows you to exit a window and terminate any unsaved changes you have made. You may also have to use this button to close a window after you have made any necessary changes and set them by clicking on an OK , Set , or Apply button.

An OK, Set, or Apply button appears in windows that have configurable values; it allows you to confirm and SET changes you have made to those values. In some windows, you may have to use this button to confirm each individual set; in other windows, you can set several values at once and confirm the sets with one click on the button.

The Help button brings up a Help text box with information specific to the current window. For more information concerning Help buttons, see **Getting Help**, page 1-6.

The command buttons, for example Bridge, call up a menu listing the windows, screens, or commands available for that topic.

Any menu topic followed by... (three dots) — for example **Statistics...** — calls up a window or screen associated with that topic.

Getting Help

This section describes two different methods of getting help for questions or concerns you may have while using NetSight Element Manager.

Using On-line Help

You can use the IRM2 window Help buttons to obtain information specific to the device. When you click on a Help button, a window will appear which contains context-sensitive on-screen documentation that will assist you in the use of the windows and their associated command and menu options. Note that if a Help button is grayed out, on-line help has not yet been implemented for the associated window.

From the **Help** menu accessed from the Chassis View window menu bar, you can access on-line Help specific to the Chassis View window, as well as bring up the Chassis Manager window for reference. Refer to **Chapter 2** for information on the Chassis View and Chassis Manager windows.

NOTE

All of the online help windows use the standard Microsoft Windows help facility. If you are unfamiliar with this feature of Windows, you can select ***Help*** *from the* Start *menu, or* ***Help —>How to Use Help*** *from the primary NetSight Element Manager window, or consult your Microsoft Windows product* **User's Guide**.

Getting Help from the Enterasys Global Call Center

If you need technical support related to NetSight Element Manager, contact the Enterasys Global Call Center via one of the following methods:

By phone:	(603) 332-9400 *24 hours a day, 365 days a year*
By mail:	Enterasys Networks Technical Support Rochester, NH 03866-5005
By Internet mail:	support@ctron.com
FTP:	ftp.ctron.com (134.141.197.25)

Login
Password
	`anonymous`
	`your email address`

By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

Send your questions, comments, and suggestions regarding NetSight documentation to NetSight Technical Communications via the following address:

Netsight_docs@enterasys.com

To locate product specific information, refer to the Enterasys Web site:

http://www.enterasys.com/.

NOTE

For the highest firmware versions successfully tested with NetSight Element Manager 2.2.1, refer to the Readme file from the NetSight Element Manager program group. If you have an earlier version of firmware and experience problems, contact the Global Technical Assistance Center.

Chapter 2

The IRM2 Chassis View

Information displayed in the Chassis View window; the physical and logical chassis views; the Chassis Manager window; Hub management functions

The IRM2 Chassis View window is the main screen that immediately informs you of the current configuration of your MMAC chassis via a graphical display of the chassis front panel. The default Logical View shows the boards installed in your MMAC according to the physical slots they occupy, and displays the condition of individual ports on those boards; the Physical View provides a graphical representation of the actual board faces. The Chassis View window serves as a single point of access to all other IRM2 windows and screens, which are discussed at length in the following chapters.

To access the IRM2 Chassis View window, use one of the following options:

1. In any map, list, or tree view, double-click on the IRM2 you wish to manage;

   or

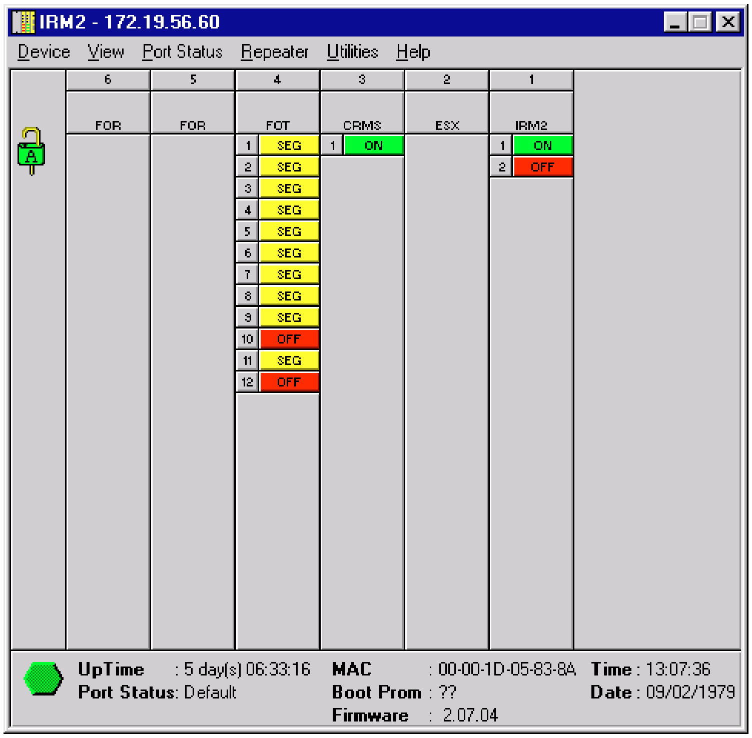
1. In any map, list, or tree view, click the **left** mouse button once to select the IRM2 you wish to manage.
2. Select **Manage—>Node** from the primary window menu bar, or select the Manage Node toolbar button.

   or

1. In any map, list, or tree view, click the **right** mouse button once to select the IRM2 you wish to manage.
2. On the resulting menu, click to select **Manage**.

Viewing Chassis Information

The IRM2 Chassis View window (Figure 2-1) provides a graphic representation of the IRM2 and the hub in which it is installed, including a color-coded port display which immediately informs you of the current configuration and status of all the boards and ports installed in the MMAC chassis.



6	5	4	3	2	1
FOR	FOR	FOT	CRMS	ESX	IRM2
		1 SEG	1 ON		1 ON
		2 SEG			2 OFF
		3 SEG			
		4 SEG			
		5 SEG			
		6 SEG			
		7 SEG			
		8 SEG			
		9 SEG			
		10 OFF			
		11 SEG			
		12 OFF			

UpTime : 5 day(s) 06:33:16
Port Status: Default
MAC : 00-00-1D-05-83-8A
Boot Prom : ??
Firmware : 2.07.04
Time : 13:07:36
Date : 09/02/1979

Figure 2-1. IRM2 Chassis View Window

By clicking in designated areas of the chassis graphical display (as detailed later in this chapter), or by using the menu bar at the top of the Chassis View window, you can access all of the menus that lead to more detailed device-, repeater-, board-, and port-level windows.

TIP

When you move the mouse cursor over a management "hot spot" the cursor icon will change into a "hand" (☝) to indicate that clicking in the current location will bring up a management option.

NOTE

Note that up to 24 ports can be displayed simultaneously on a module. If a module has a higher port density than 24 ports, Up and Down arrows will appear at the top and bottom of the port stack so that you can scroll through the remaining ports.

Front Panel Information

The areas outside the main MIM display area provide the following device information:

IP

The Internet Protocol address assigned to the IRM2; this field will display the IP address you have used to create the IRM2 icon. IP addresses are assigned via Local Management.

Port Locking/Unlocking

The port locked and unlocked symbols indicate whether port locking is enabled or disabled, respectively. See Chapter 4, **Source Address Functions**, for further information.

Connection Status

This color-coded area indicates the current state of communication between NetSight Element Manager and the IRM2.

- **Green** indicates the IRM2 is responding to device polls (valid connection).
- **Magenta** indicates that the IRM2 is in a temporary stand-by mode while it responds to a physical change in the hub (a board is inserted or removed); note that board and port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status — polling has not yet been established with the IRM2.
- **Red** indicates the IRM2 is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

UpTime

The amount of time, in a days hh:mm:ss format, that the IRM2 has been running since the last start-up.

Port Status

If management for your device supports a variable port display (detailed in **Port Status Displays** later in this chapter), this field will show the display currently in effect. If only a single port display is available--or if the default view is in effect--this field will state **Default**.

MAC

The physical layer address assigned to the IRM2 interface with which NetSight Element Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

Boot Prom

The revision of BOOT PROM installed in the IRM2.

Firmware

The revision of device firmware stored in the IRM2's FLASH PROMs.

Time

The current time, in a 24-hour hh:mm:ss format, set in the IRM2's internal clock.

Date

The current date, in an mm/dd/yyyy format, set in the IRM2's internal clock.

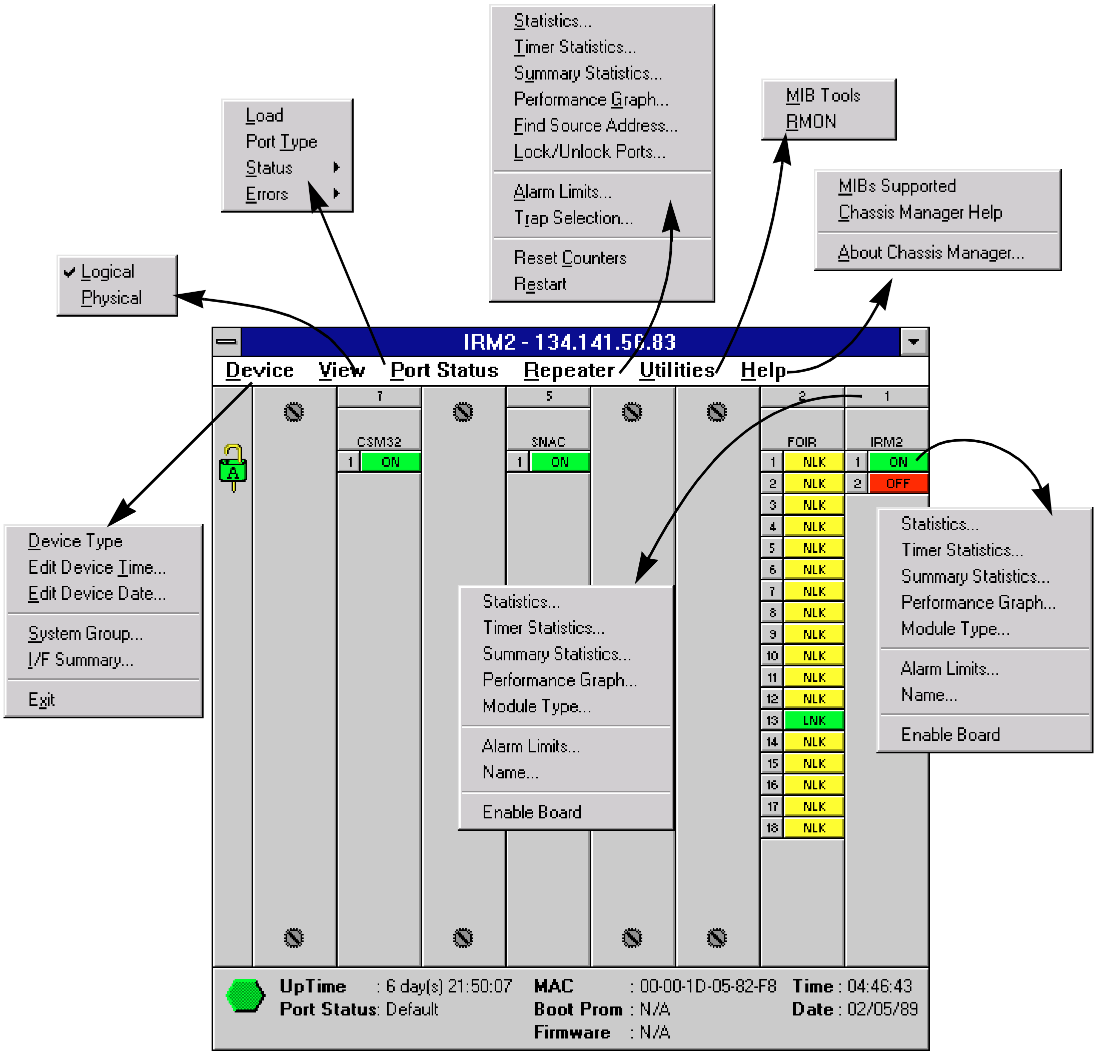
NOTE

You can set the date and time by using the ***Edit Device Date*** *and* ***Edit Device Time*** *options on the Device menu, or by using the I-bar cursors in the Chassis Type window; see* ***Setting the Device Date and Time****, page 2-14****,*** *f or details.*

In accordance with Year 2000 compliance requirements, NetSight Element Manager now displays and allows you to set all date s with four-digit year values..

Menu Structure

By clicking on various areas of the IRM2 Chassis View display, you can access menus with device-, repeater-, board-, and port-level options, as well as utility applications which apply to the device. The following illustration displays the menu structure and indicates how to use the mouse to access the various menus:



UpTime : 6 day(s) 21:50:07
Port Status: Default
MAC : 00-00-1D-05-82-F8
Boot Prom : N/A
Firmware : N/A
Time : 04:46:43
Date : 02/05/89

Figure 2-2. IRM2 Chassis View Menu Structure

The Device Menu

From the Device Menu at the Chassis View window menu bar, you can access the following selections:

- **Device Type...**, which displays a window containing a description of the device being modeled (i.e., IRM2).
- **Edit Device Time...** and **Edit Device Date...**, which allow you to set the IRM2's internal clock.
- **System Group...**, which allows you to manage the IRM2 via SNMP MIB II. Refer to the ***Generic SNMP User's Guide*** for further information.

- **I/F Summary**, which displays a window showing statistics for the traffic processed by each network interface on your device. Refer to **Viewing I/F Summary Information**, page 2-18.
- **Exit**, which closes the IRM2 Chassis View window.

The View Menu

The View menu lets you change the information displayed in the Chassis View:

- **Logical** brings up the default display, which contains port status information and provides access to board- and port-level menus.
- **Physical** provides a graphic representation of the actual module faces, showing how ports are arranged on the MIM face and what connector types are present.
- **Redundancy** brings up a window that allows you to configure a redundancy scheme for the IRM2 and its associated modules. See Chapter 7, **Redundancy**, for further information.

The Port Status Menu

The Port Status menu allows you to select the status information that will be displayed in the port text boxes in the logical Chassis View window:

- **Load** will display the portion of network load processed by each port as a percentage of the theoretical maximum load (10Mbits/sec) of an Ethernet network.
- **Port Type** will display each port’s topology: Station (STA) or Trunk (TRK).
- **Status** allows you to select one of three status type displays: **Admin/Link**, **Admin**, or **Link**.
- **Errors** allows you to display the percentage per port of the specific Error type you select.

For more information on the port display options available via this menu, see **Selecting a Port Status View**, in this chapter.

The Repeater Menu

This menu displays selections pertaining to the repeater network supported by the IRM2. It has the following selections:

- **Statistics...**, which brings up the repeater-level Statistics windows; see Chapter 3, **Statistics**, for more information.
- **Timer Statistics...**, which opens the repeater-level Timer Statistics windows; see **Chapter 3** for more information.
- **Summary Statistics...**, which accesses repeater-level statistics broken down by individual board; see **Chapter 3**.
- **Performance Graph...**, which opens the Performance Graph windows; see **Chapter 3**.

- **Find Source Address...**, which allows you to locate the port through which a MAC address is communicating; see Chapter 4, **Source Address Functions**.
- **Lock/Unlock Ports...**, which allows you to protect the hub from unauthorized access; see Chapter 4, **Source Address Functions**.
- **Alarm Limits...**, which launches the repeater-level alarms window; see Chapter 5, **Alarm Limits**, for alarm configuration information.
- **Trap Selection...**, which allows you to selectively enable and disable certain SNMP traps generated by the IRM2; see Chapter 6, **Trap Selection**.
- **Reset Counters**, which lets you refresh the IRM2's statistical counters to zero. This option is discussed later in this chapter.
- **Restart...**, which you can use to perform a warm boot of the IRM2. This option is discussed later in this chapter.

The Utilities Menu

The Utilities menu provides access to any utilities provided by NetSight Element Manager for use with the IRM2 module. This includes the MIB Tree utility, which provides direct access to the IRM2's MIB information. Refer to your ***Utilities User's Guide*** for information on this utility.

The Help Menu

The Help Menu has three selections:

- **Mibs Supported**, which brings up the Chassis Manager window, described later in this chapter.
- **Chassis Manager Help**, which brings up a help window with information specifically related to using the Chassis Manager and Chassis View windows.
- **About Chassis Manager...**, which brings up a version window with the Chassis Manager application in use.

The Board Menu

The Board menu for the IRM2 module and its associated modules provides the following selections. If the board you are monitoring is not recognized by the IRM2 — for example, if it is a mid-chassis intelligent module such as a GatorMIM — the single board-level selection available is **Module Type...**:

- **Statistics...** (see Chapter 3)
- **Timer Statistics...** (see Chapter 3)
- **Summary Statistics...** (see Chapter 3)
- **Performance Graph...** (see Chapter 3)
- **Module Type...**, which brings up a window containing a description of the selected board; see **Viewing Hardware Types**, page 2-13.
- **Alarm Limits...** (see Chapter 5)

- **Name...**, which allows you to assign a name to the selected board; this name will be displayed in many board-level windows. See **Setting a Board Name**, page 2-17, for details.
- **Enable**, which allows you to enable all ports on the selected board; see **Enabling Boards**, page 2-17.

The Port Menus

For Ethernet MIM ports, menu selections will include **Statistics**, **Timer Statistics**, **Performance Graph**, and **Alarm Limits** (the same options provided on the repeater and board menus); **Enable** and **Disable** at the port level; and an additional port-specific selection:

- **Source Addressing...**, which displays the current source address table for each port. See Chapter 4, **Source Address Functions**, for more information.

The IRM2 Module itself (Board 1) has one additional port-related option:

- **Port Association...**, which lets you select which of its two front panel ports — AUI or Fiber Optic —þwill be used as the repeater interface for a connected network segment.

MIM Port Status Displays

When you open the Chassis View window, each port on the IRM2 and the associated MIMs installed in the hub will display its Admin/Link status (defined below); to change this status display, select one of the options on the Port Status menu, as described in the following sections.

Selecting a Port Status View

To change the status view of your ports:

1. Click on **Port Status** on the menu bar at the top of the Chassis View window; a menu will appear.
2. Drag down (and to the right, if necessary) to select the status information you want to display. The port text boxes will display the appropriate status information.

Port status view options are:

Load

If you choose **Load**, the port text boxes will display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated by devices connected to the port compared to the theoretical maximum load (10 Mbits/sec) of an Ethernet network.

*In NetSight Element Manager, the polling interval is set via the **Tools—>Options** window available from the primary window menu bar.*

*Refer to the **NetSight Element Manager User’s Guide f**or full information on setting device polling intervals.*

Port Type

If you choose **Port Type**, each port status box will display that port’s topology status: station or trunk. A station port (displayed as STA) is one which has zero or one source addresses in its source address table; a trunk port (designated TRK) has two or more source addresses in its table. If a board does not support the Port Type option, its port status boxes will remain blank. For more information about the source address table, see Chapter 4, **Source Address Functions**.

Status

You can view three status categories for your ports, which reflect six possible Admin/Link, Admin, or Link status conditions:

- **Admin/Link** — ON, OFF, SEG (segmented), or NLK (not linked)
- **Admin** — ON or OFF
- **Link** — LNK (link), NLK (not linked), or N/A (not available)

If you have selected the **Admin/Link** status mode, a port is considered:

- ON if the port is enabled and has a valid link.
- OFF if it has not been enabled or if it has been disabled through management action.

SEG (segmented) if the port has been enabled by management and has a valid connection, but has been segmented by the repeater because 33 consecutive collisions have occurred on the attached segment, or the collision detector was on for more than 2.4 µs.

NOTE

Because BNC thin coax and AUI ports do not support the link feature, the displayed Admin/Link, Admin, and Link status conditions will not always follow the pattern described above.

*Under **Admin/Link** status mode, BNC ports will display as ON if there is a valid connection and the port has been enabled; OFF if the port has been disabled; and SEG if the port has experienced 33 consecutive collisions or if there is no cable attached. An AUI port will display as ON if the port has been enabled (regardless of whether or not there is a valid connection), OFF if the port has been disabled, and SEG if the port has detected 33 consecutive collisions. Note that the Admin/Link status displays for BNC and AUI ports can be misleading in terms of troubleshooting; be sure to keep in mind that a BNC port displaying as segmented may only have had its cable disconnected, and an AUI port that appears to be on and linked may not have any cable attached.*

*Under **Admin** status mode, AUI and BNC ports will display as ON if the port has been enabled, and OFF if it has been disabled; as with other port types, these ON and OFF conditions indicate nothing about link status.*

*Under **Link** status mode, AUI and BNC port display boxes will display N/A, indicating that NetSight Element Manager is unable to determine their link status.*

- NLK (Not Linked) when the port is on, but there is no physical link to the port. This field is a combination of two status conditions: No Link and Port Administrative Status On.

If you have selected the **Admin** status mode, a port is considered:

- ON if the port is enabled.
- OFF if the port has been disabled by management.

Note that these conditions do not reflect *link* status.

If you have selected the **Link** status mode, a port is considered:

- LNK (Linked) when a valid link has been established between the port and the device at the other end of the segment.
- NLK (Not Linked) when the port is on, but there is no physical link to the port or the device at the other end of the port’s segment is down.
- N/A (not available) when NetSight Element Manager cannot determine the link status for the port.

Errors

If you choose the **Errors** mode, an additional menu offers the following options:

- Total Errors, Collisions, Alignment, CRC, Runts, Giants, or OOW Coll.

Select one of the **Errors** options to see what percentage of the total packets received by each active port during the last polling interval was of the error type you selected. This percentage reflects the number of errors generated by devices connected to that port in relation to the total number of packets processed by the port (errors ÷ [errors + packets]).

Port Status Color Codes

Two of the port status display options — Port Type and Status — incorporate their own color coding schemes, as described below:

- For any of the **Status** display options — Admin / Link, Admin, or Link — green = ON / LNK, yellow = SEG / NLK, red = OFF, and blue = N / A (not available).
- For the **Port Type** display option, station ports will display as yellow; trunk ports will display as green.

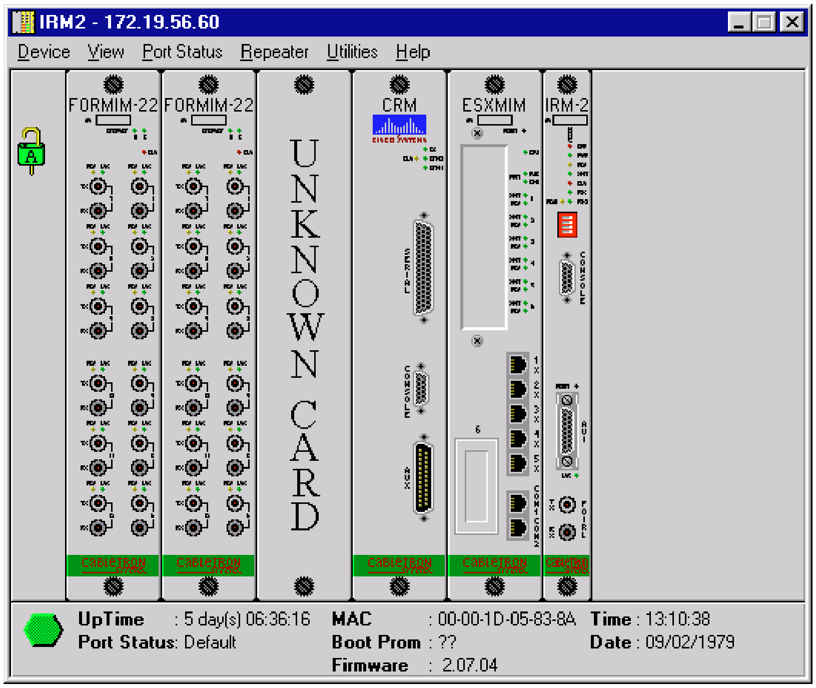
For the other Port Status selections — **Load** and **Errors —** color codes will continue to reflect the most recently selected mode which incorporates its own color coding scheme.

The Physical Chassis View

By default, the Chassis View window displays a Logical View of the hub and its installed modules; the Logical View provides port status information and access to repeater-, board-, and port-level menus, as described above. In addition to the default logical view, however, the View menu available via the menu bar at the top of the Chassis View window allows you to display a Physical View of the Hub and the actual faces of the installed modules. While the Physical View does not provide any port status information or access to board- or port-level menus, it serves as a useful tool for network managers who are physically remote from the devices they are managing and who need to see the arrangement of ports on the MIM face and the connector types supported.

To access the Physical View:

1. In the Chassis View window, click on **View** in the menu bar to access the View menu.
2. Drag down to **Physical**, and release. The Chassis Physical View, Figure 2-3, will appear.
3. To switch back to the Logical view, select **Logical** from the menu, and release.



UpTime : 5 day(s) 06:36:16
Port Status: Default

MAC : 00-00-1D-05-83-8A
Boot Prom : ??
Firmware : 2.07.04

Time : 13:10:38
Date : 09/02/1979

Figure 2-3. The Physical Chassis View

The Chassis Manager Window

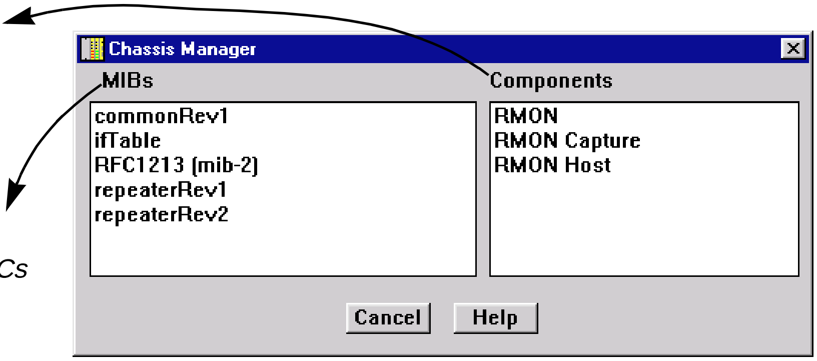
Like most networking devices, Enterasys’ and Cabletron’s devices draw their functionality from a collection of proprietary MIBs and IETF RFCs. The Chassis Manager window, Figure 2-4, is a read-only window that displays the MIBs and the MIB components — and, therefore, the functionality — supported by the currently monitored device.

To view the Chassis Manager window:

1. Click on **Help** on the menu bar at the top of the Chassis View window.
2. Drag down to **MIBs Supported**, and release.

MIB Components are listed here; for first generation devices like the IRM2, all MIB information is organized into a single component

The MIBs which provide the IRM2's functionality — both proprietary MIBs and IETF RFCs — are listed here



Chassis Manager

MIBs

commonRev1
ifTable
RFC1213 (mib-2)
repeaterRev1
repeaterRev2

Components

RMON
RMON Capture
RMON Host

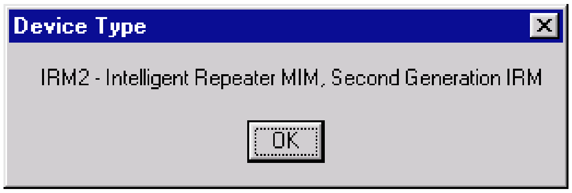
Figure 2-4. Chassis Manager Window

Viewing Hardware Types

In addition to the graphical displays described above, menu options available at several levels provide specific information about the physical characteristics of modules and ports in the IRM2-controlled hub, as well as information about the hub itself.

Device Type

Choosing the **<u>D</u>evice Type...** option on the Device menu brings up a window that describes the management device being modeled:



Device Type

IRM2 - Intelligent Repeater MIM, Second Generation IRM

Figure 2-5. Sample Device Type Window

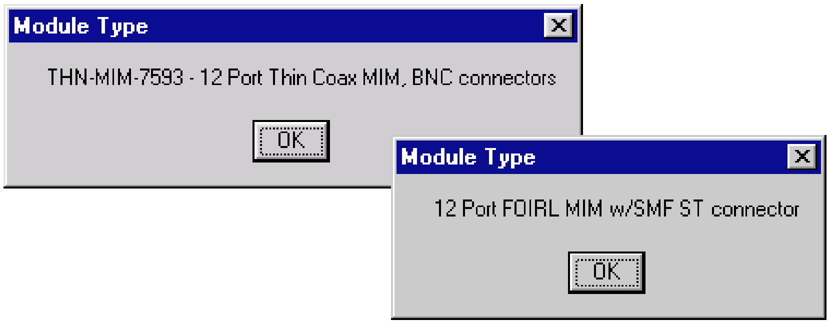
Module Type

From the Board menus on the IRM2 Chassis View window, you can view a description of the Module types in your IRM2-controlled MMAC.

To view a Module Type:

1. Click on the desired **Board** number. The Board menu will appear.

2. Drag down to **Module Type...**. A Module Type text box, similar to the examples shown in Figure 2-6, will appear describing the board type. If Module Type is not supported by the selected board, “Unknown” will appear in the text box.



Module Type

THN-MIM-7593 - 12 Port Thin Coax MIM, BNC connectors

Module Type

12 Port FOIRL MIM w/SMF ST connector

Figure 2-6. Sample Module Type Text Boxes

Managing the Hub

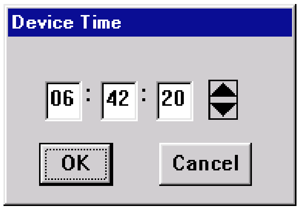
In addition to the performance and configuration information described in the preceding sections, the Chassis View also provides you with the tools you need to configure your hub and keep it operating properly. Hub management functions include setting device date and time, configuring the IRM2 front panel repeater port, setting board names, and enabling and disabling ports.

Setting the Device Date and Time

You can select the **Edit Device Time** and **Edit Device Date** options from the Device menu to change the date and time stored in the device’s internal clock.

To edit the device time:

1. Click on **Device** on the Chassis View window menu bar to access the Device menu; drag down to **Edit Device Time...**, and release. The following change window, Figure 2-7, will appear.



Device Time

06 : 42 : 20

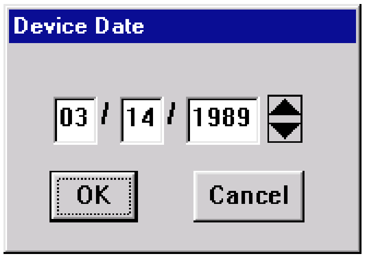
Figure 2-7. Edit Time Window

2. Enter the new time in a 24-hour hh:mm:ss format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.

3. Click on OK to save your changes, or on to cancel.

To edit the device date:

1. Click on **<u>D</u>evice** on the Chassis View window menu bar to access the Device menu; drag down to **<u>E</u>dit Device Date...**, and release. The following change window, Figure 2-8, will appear.



03 / 14 / 1989

Figure 2-8. Edit Date Window

2. Enter the new date in a mm/dd/yy format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.

3. Click on OK to save your changes, or on to cancel

.

NOTE

In accordance with Year 2000 compliance requirements, NetSight Element Manager now displays and allows you to set all date s with four-digit year values..

Resetting Device Counters

To refresh statistics totals, you can reset counter information for your IRM2 back to zero. To do so:

1. Select **<u>R</u>epeater** from the Chassis View menu; drag down to **Reset Counters** and release.

Restarting the Device

You can use the Restart Device option to perform a warm boot of the IRM2. This will reset all counter information to zero and refresh system uptime.

To do so:

1. Select **Repeater** from the Chassis View menu; drag down to **Restart...** and release.

The IRM2 will be restarted as if it had just been powered up.

Configuring the Front Panel Repeater Port Association

Using the Port Association option for the IRM2, you can set which of the IRM2's front panel ports will act as a repeater interface for a connected network segment.

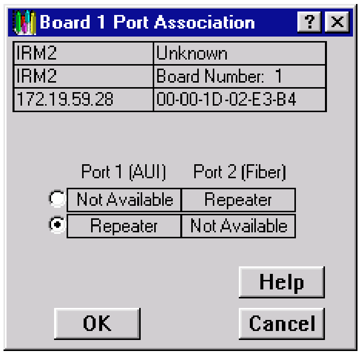
CAUTION

Before selecting this option, be sure that you will not disrupt network activity. If you disconnect the segment with which you are communicating with the IRM2, you will lose contact with the device, and you will have to reset the original port association through local management.

To change the port association:

1. Click on **Port 1** or **Port 2** on Board 1 (the IRM2 module). The Port pull-down menu will appear.

2. Click on **Port Association...**. The Port Association window, Figure 2-9, will appear.



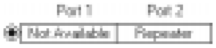
Board 1 Port Association

IRM2	Unknown
IRM2	Board Number: 1
172.19.59.28	00-00-1D-02-E3-B4

	Port 1 (AUI)	Port 2 (Fiber)
○	Not Available	Repeater
●	Repeater	Not Available

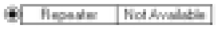
Figure 2-9. Repeater Port Association

Click on the appropriate radio button:



	Port 1	Port 2
●	Not Available	Repeater

indicates that Port 2 (the Fiber Optic Link Port) will be made the active repeater interface for an attached fiber segment, and that Port 1 (the AUI Port) will be disabled.



●	Repeater	Not Available

indicates that Port 1(the AUI port) will be used to repeat data from its attached network segment, and Port 2 (Fiber Optic Link Port) will be disabled.

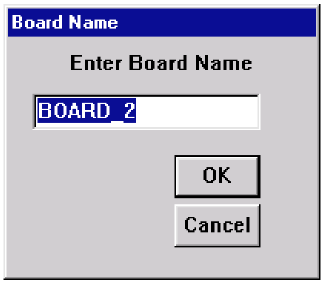
3. Click on OK . The selected port association will take effect; one port will become the active repeater interface and the other will be administratively disabled. The Chassis View display for the IRM2 module will update to reflect the change.

Setting a Board Name

From the Board menus on the Chassis View window, you can change the names of the manageable boards installed in your MMAC.

To name a board:

1. Click on the appropriate **Board** number to access the board menu.
2. Drag down to **Name...**. The Board Name Text Box, Figure 2-10, will appear.



Enter Board Name

BOARD_2

Figure 2-10. Board Name Text Box

3. Enter the name of the board, up to 20 characters in length.
4. Click on OK .

Your new name will be applied to the board, and will appear in a number of board-related windows.

Enabling Boards

From the Board menus in the Chassis View window, you can enable any manageable boards in your MMAC that are currently disabled by management.

To enable a board:

1. Click on the desired **Board** number to access the board menu.
2. Drag down to **Enable**. Your board will now be enabled, and the port status for disabled ports will change from OFF to the appropriate status (ON, SEG, LNK, or NLK).

Enabling and Disabling Ports

From the Port menus on the IRM2 Chassis View window, you can enable and disable any individual ports.

To enable or disable a port:

1. Click on the desired **Port** button. The Port menu will appear.
2. Click on **Enable** to enable the port, or **Disable** to disable the port. Your port will now be enabled or disabled as desired.

NOTE

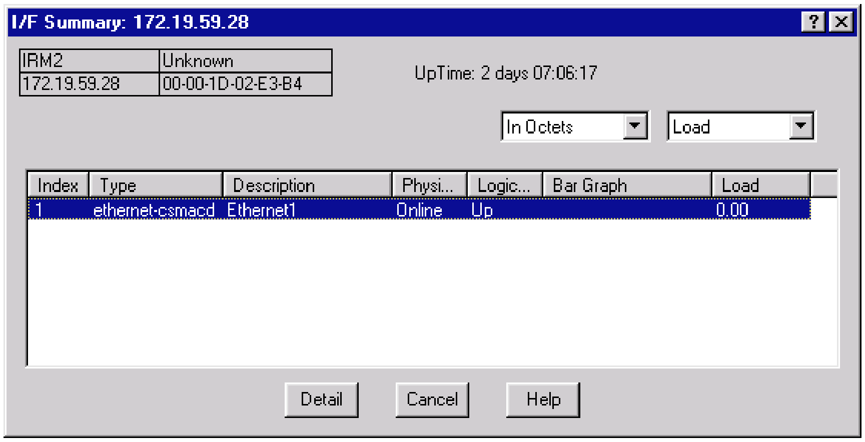
You must use this port enabling feature to re-enable ports that were formerly part of a redundant circuit, or ports that have been shut down in response to port locking or due to an alarm condition. Consult Chapter 5, ***Alarm Limits****, and Chapter 7,* ***Redundancy****, for more information.*

Viewing I/F Summary Information

The **I/F Summary** menu option available from the Device menu lets you view statistics for the traffic processed by each network interface on your device. The window also provides access to a detailed statistics window that breaks down Transmit and Receive traffic for each interface.

To access the I/F Summary window:

1. From the Module View, click on the **Device** option from the menu bar.
2. Click again to select **I/F Summary**, and release. The I/F Summary window, Figure 2-11, will appear.



I/F Summary: 172.19.59.28

IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

UpTime: 2 days 07:06:17

In Octets

Load

Index	Type	Description	Physi...	Logic...	Bar Graph	Load
1	ethernet-csmacd	Ethernet1	Online	Up		0.00

Figure 2-11. I/F Summary Window

The I/F Summary window provides a variety of descriptive information about each interface on your device, as well as statistics which display each interface's performance.

The following descriptive information is provided for each interface:

UpTime

The **UpTime** field lists the amount of time, in a days, hh:mm:ss format, that the device has been running since the last start-up.

Index

The index value assigned to each interface on the device.

Type

The type of the interface, distinguished by the physical/link protocol(s) running immediately below the network layer.

Description

A text description of the interface

Physical Status

Displays the current physical status — or operational state — of the interface: **Online** or **Offline**.

Logical Status

Displays the current logical status — or administrative state — of the interface: **Up** or **Down**.

Interface Performance Statistics/Bar Graphs

The statistical values (and, where available, the accompanying bar graphs) to the right of the interface description fields provide a quick summary of interface performance. You can select the statistical value you want to display and the units in which you want those values displayed by using the two menu fields directly above the interface display area, as follows:

1. In the right-most menu field, click on the down arrow and select the unit in which you wish to display the selected statistic: **Load**, **Raw Counts**, or **Rate**.

NOTE

*Bar graphs are only available when **Load** is the selected base unit; if you select **Raw Counts** or **Rate**, the Bar Graph column will be removed from the interface display.*

2. Once you have selected the base unit, click on the down arrow in the left-most field to specify the statistic you'd like to display. Note that the options available from this menu will vary depending on the base unit you have selected.

After you select a new display mode, the statistics (and graphs, where applicable) will refresh to reflect the current choice, as described below.

Raw Counts

The total count of network traffic received or transmitted on the indicated interface since device counters were last reset. Raw counts are provided for the following parameters:

In Octets

Octets received on the interface, including framing characters.

In Packets

Packets (both unicast and non-unicast) received by the device interface and delivered to a higher-layer protocol.

In Discards

Packets received by the device interface that were discarded even though no errors prevented them from being delivered to a higher layer protocol (e.g., to free up buffer space in the device).

In Errors

Packets received by the device interface that contained errors that prevented them from being delivered to a higher-layer protocol.

In Unknown

Packets received by the device interface that were discarded because of an unknown or unsupported protocol.

Out Octets

Octets transmitted by the interface, including framing characters.

Out Packets

Packets transmitted, at the request of a higher level protocol, by the device interface to a subnetwork address (both unicast and non-unicast).

Out Discards

Outbound packets that were discarded by the device interface even though no errors were detected that would prevent them from being transmitted. A possible reason for discard would be to free up buffer space in the device.

Out Errors

Outbound packets that could not be transmitted by the device interface because they contained errors.

Load

The number of bytes processed by the indicated interface during the last poll interval in comparison to the theoretical maximum load for that interface type (10 Mbps for standard Ethernet). Load is further defined by the following parameters:

In Octets

The number of bytes received by this interface, expressed as a percentage of the theoretical maximum load.

Out Octets The number of bytes transmitted by this interface, expressed as a percentage of the theoretical maximum load.

When you select this option, a Bar Graph field will be added to the interface display area; this field is only available when **Load** is the selected base unit.

Rate

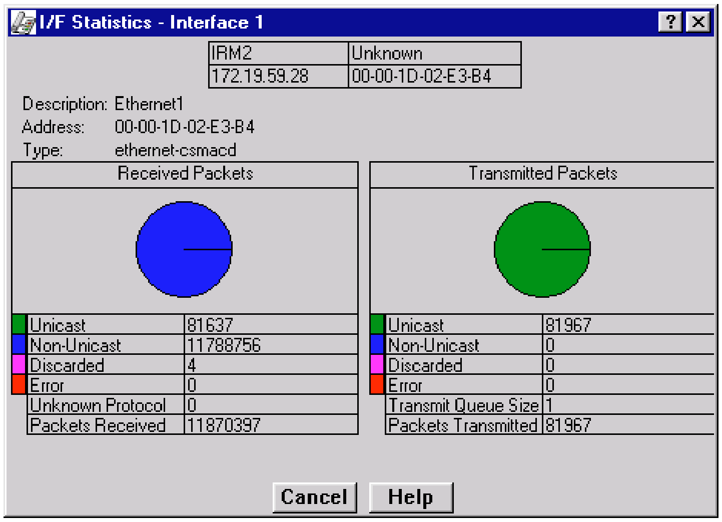
The count for the selected statistic during the last poll interval. The available parameters are the same as those provided for Raw Counts. Refer to the Raw Counts section, above, for a complete description of each parameter.

Viewing Interface Detail

The Interface Statistics window (Figure 2-12) provides detailed MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for each individual port. Color-coded pie charts also let you graphically view statistics for both received and transmitted Unicast, Multicast, Discarded, and Error packets.

To open the Interface Statistics window:

1. In the I/F Summary window, click to select the interface for which you'd like to view more detailed statistics.
2. click on **Detail**. The appropriate I/F Statistics window, Figure 2-12, will appear.



IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

Description: Ethernet1
Address: 00-00-1D-02-E3-B4
Type: ethernet-csmacd

Received Packets

🟩	Unicast	81637
🟦	Non-Unicast	11788756
🟪	Discarded	4
🟥	Error	0
	Unknown Protocol	0
	Packets Received	11870397

Transmitted Packets

🟩	Unicast	81967
🟦	Non-Unicast	0
🟪	Discarded	0
🟥	Error	0
	Transmit Queue Size	1
	Packets Transmitted	81967

Figure 2-12. Detail Interface Statistics

TIP *You can also access this information via the I/F Statistics option available on the individual port menus; see Chapter 3* ***Statistics****, for more information.*

Three informational fields appear in the upper portion of the window:

Description
Displays the interface description for the currently selected interface: Ethernet.

Address
Displays the MAC (physical) address of the selected interface.

Type
Displays the interface type of the selected port: ethernet-csmacd.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast
Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast
Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The multicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded
Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges or switches.

These statistics are displayed in the pie chart, color-coded magenta.

Error
Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol *(Received only)*
Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received *(Received only)*
Displays the number of packets received by the selected interface.

Transmit Queue Size *(Transmit only)*
Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the 9H42x-xx module will begin to discard packets.

Packets Transmitted *(Transmit only)*
Displays the number of packets received by the selected interface.

Making Sense of Detail Statistics

The statistics available in this window can give you an idea of how an interface is performing; by using the statistics in a few simple calculations, it's also possible to get a sense of an interface's activity level:

To calculate the percentage of input errors:

```
Received Errors /Packets Received
```

To calculate the percentage of output errors:

```
Transmitted Errors /Packets Transmitted
```

To calculate the total number of inbound and outbound discards:

```
Received Discards + Transmitted Discards
```

To calculate the percentage of inbound packets that were discarded:

```
Received Discards /Packets Received
```

To calculate the percentage of outbound packets that were discarded:

```
Transmit Discards /Packets Transmitted
```

NOTE

Unlike the Interface Detail window, which this window replaces, the Interface Statistics window does not offer ***Disable*** *or* ***Test*** *options. These options are available in the Interface Group window, which can be accessed via the System Group window (select* ***System Group...*** *from the* ***Device*** *menu). Refer to your* **Generic SNMP User's Guide** *for further information on the System Group and Interface Group windows.*

Testing and Disabling the Current Interface

With the Test button you can test the current interface (e.g., by performing a loopback or some other transmission test).

With the Test and Disable buttons, you can test or disable the current interface. The operational states of these two options are:

Test — The interface will be in some test mode and no operational packets can be passed.

Disable — The interface will be in a closed state.

TIP

The Test and Enable/Disable buttons attempt to set the ifAdmin Status OID to the Enable, Disable, or Test values. Not all device firmware will allow you to perform a SET of this MIB OID for all interfaces, so attempts to test or enable/disable an interface may result in a SET FAILED message.

To test the current interface:

1. Click on . The current interface will now be operating in the test state.

To disable the current interface:

1. Click on Disable. The current interface will now be operating in a closed state.

Using the Applications menu

The Applications button leads you to a menu that indicates device-associated SNMP MIB-I or MIB-II functions that the device supports.

To access the Applications pull-down menu:

1. Using the mouse, click on . A menu will appear with SNMP-MIB II options supported by the device; non-supported options will be grayed out.
2. Click on the desired option. The appropriate window will appear.

Chapter 3

Statistics

Accessing the Statistics, Timer Statistics, Summary Statistics, and Performance Graph windows; statistics defined; using the Total and Delta radio buttons; setting the Timer Statistics time interval; configuring the performance graphs

The statistical information collected and stored by your IRM2 provides you with detailed information about how much traffic your network (or a segment thereof) is experiencing, including the sizes and types of packets that make up that traffic, and how much of that traffic comprises packets which have been badly formed or somehow mangled in transmission. These statistics can give you a good overall sense of the usage your network, or network segment, is experiencing.

To help you better understand and track the traffic your network is handling, NetSight Element Manager's main provides you with a variety of statistical information presented in four different formats: Statistics, Timer Statistics, Summary Statistics, and Performance Graphs.

Statistics

At the Statistics windows, you can view accumulated statistics and error breakdowns for the device as a whole and for each individual board and/or port. A pie chart graphically depicts these statistics for quick visual reference.

Statistics displayed in these windows include:

- Active Users
- Bytes
- Broadcasts
- Packets

The Active Users and Broadcasts selections are ***not*** *available for early generation IRM2s equipped with pre-version 2.00 release firmware.*

- Transmit Collisions
- Receive Collisions

- Out-of-Window (OOW) Collisions
- Giant Packets

- Alignment Errors
- CRC Errors
- Runts

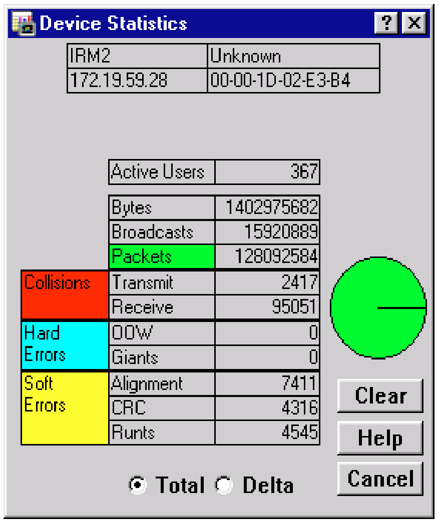
The pie chart to the right of the statistics lets you graphically view your statistics. The colors in the pie chart correspond to the colors for Packets (green), Collisions (red), and the two error modes: Hard Errors (blue) and Soft Errors (yellow).

Accessing the Statistics Windows

To access the Repeater Statistics window:

1. Click on **Repeater** on the Chassis View menu bar to display the repeater menu.

2. Drag down to **Statistics...** and release. The Repeater Statistics window, Figure 3-1, will appear.



Device Statistics

IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

	Active Users	367
	Bytes	1402975682
	Broadcasts	15920889
	Packets	128092584
Collisions	Transmit	2417
	Receive	95051
Hard Errors	OOW	0
	Giants	0
Soft Errors	Alignment	7411
	CRC	4316
	Runts	4545

● Total ○ Delta

Figure 3-1. Statistics Window

To open the board-level Statistics window:

1. Click on the appropriate **Board number** to display the board menu.
2. Drag down to **Statistics...** and release. The board-level Statistics window will appear.

To access the port-level Statistics window:

1. Click on the appropriate **Port** to display the port menu.
2. Drag down to **Statistics...** and release. The port-level Statistics window will appear.

The Board and Port Statistics windows are the same as the Statistics window displayed in Figure 3-1, except that they display statistics applicable to the selected board or port.

Statistics Defined

The statistics window displays the statistical counts accumulated since the IRM2 was last reset or since the last time the Clear button was selected. You can select Clear at any time to refresh the counters and restart at zero.

The statistics windows display the following information:

Active Users (Available with Release Version 2.00 Firmware and Above)

Displays the number of users (identified by MAC [Ethernet] address) communicating via a port on the IRM2-managed hub. For an individual port, if Active Users is greater than one, it indicates that a port is supporting a trunk connection and will not respond to port locking. Refer to Chapter 4, **Source Address Functions**, in this guide for more information.

Bytes

Displays the total number of bytes (good packets only) that have been processed by the device, board, or port. Note that this byte count does **not** include errors.

Broadcasts (Available with Release Version 2.00 Firmware and Above)

Displays the total number of broadcast frames that have been processed by the device, board, or port. Broadcast packets have a single address recognized by each station on the net; this address is designated in IP address form as 255.255.255.255, or in MAC hexadecimal form as FF-FF-FF-FF-FF-FF. ARP and RARP requests sent by bridges and routers are broadcast messages.

Packets

Displays the total number of good packets processed by the device, board, or port. Again, note that the packet count does **not** include errors.

Collisions

Transmit

Displays the number of transmit collisions detected by the device, board, or port. Transmit collisions are those the IRM2 detects while transmitting a packet, which means the IRM2 has transmitted one of the colliding packets.

Receive

Displays the number of receive collisions detected by the device, board, or port. Receive collisions are those detected by the IRM2 while it is receiving a transmission.

Hard Errors

OOW Collisions

Displays the number of collisions out of the standard collision window (51.2 µs) experienced by the device, board, or port. Out-of-window collisions typically indicate a network design flaw.

Giants

Displays the number of giant packets that the device, board, or port has received from the network. A giant packet exceeds the maximum Ethernet frame size of 1518 bytes (excluding the preamble).

Soft Errors

Alignment Errors

Displays the total number of misaligned packets received by the device, board, or port. A misaligned packet is one that contains a non-integral number of bytes (that is, any unit of bits less than a byte). Alignment errors are also known as framing errors.

CRC Errors

Displays the total number of packets with CRC (**C**yclical **R**edundancy **C**heck) errors that the device, board, or port has received from the network. CRC errors occur when packets are somehow damaged in transit.

Runts

Displays the number of runt packets that the device, board, or port has received from the network. A runt packet is one that is less than the minimum Ethernet frame size of 64 bytes.

Using the Total and Delta Radio Buttons

By using the **Total** and **Delta** radio buttons located at the bottom of the Statistics windows, you can choose whether to view the total statistics count (**Total**) or the statistics count for the last polling interval (**Delta**).

To choose Total or Delta:

1. Click on the **Total** radio button; after the completion of the current polling cycle plus one complete polling cycle, the screen will display the total count of statistics processed since the most recent start-up of the IRM2.

2. Click on the **Delta** radio button; after the completion of the current polling cycle plus two more polling cycles, the screen will display the count of statistics processed during the last poll interval. These counts will be refreshed after each polling interval.

   ■ — indicates that the associated option is **not** chosen

   ■ — indicates that the associated option **is** chosen

Timer Statistics

You can use the Timer Statistics windows to gather statistical information concerning your IRM2 and its boards and / or ports over a user-set time period. Statistics are displayed both numerically and graphically, using color-coded, dynamic bar charts. These bar charts display the elapsed, average, and peak values for packets, errors, and bytes at the device, board, or port level. The values are color-coded as follows:

- **Green** (Elapsed) — Indicates the level of activity during the last time interval.
- **Blue** (Average) — Indicates the average levels of activity over all timer intervals since the window was invoked.
- **Magenta** (Peak) — Indicates the peak level of activity over all time intervals since the window was invoked.

The displayed statistics will automatically update using the time interval you have set; allowable time intervals range from one second to 23 hours / 59 minutes / 59 seconds. You can also refresh the statistics accumulated in the Timer Statistics window at any time by clicking **Clear**. This will only reset the counters at the Timer Statistics window; the statistical counts maintained by the device are not affected. The time under the **Clear** button will also update, indicating the last time that the Timer Statistics window was cleared.

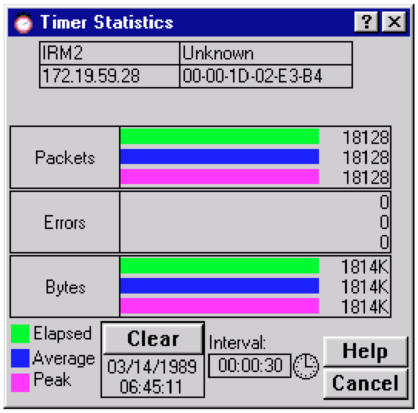
NOTE

The time interval set in the Timer Statistics window functions independently from the polling interval you have set for your software during installation.

Accessing the Timer Statistics Windows

To access the Repeater Timer Statistics window:

1. Click on **Repeater** on the Chassis View menu bar to display the repeater menu.
2. Drag down to **Timer Statistics...** and release. The Repeater Timer Statistics window, Figure 3-2, will appear.



IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

Packets	18128 18128 18128
Errors	0 0 0
Bytes	1814K 1814K 1814K

03/14/1989 06:45:11

Interval: 00:00:30

Figure 3-2. Timer Statistics Window

To open the board-level Timer Statistics window:

1. Click on the appropriate **Board number** to display the board menu.
2. Drag down to **Timer Statistics...** and release. The board-level Statistics window will appear.

To access the port-level Timer Statistics window:

1. Click on the appropriate **Port** to display the port menu.
2. Drag down to **Timer Statistics...** and release. The port-level Statistics window will appear.

The Board and Port Timer Statistics windows are the same as the Timer Statistics window displayed in Figure 3-2, except that they display statistics applicable to the board or port.

The Timer Statistics windows display the elapsed, average, and peak values for the following statistics:

Packets

Displays the elapsed, average, and peak number of good packets processed by the device, board, or port during the user-defined time interval.

Errors

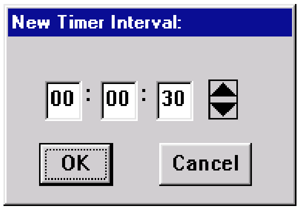
Displays the elapsed, average, or peak number of errors received by the device, board, or port during the user-defined time interval.

Bytes
Displays the elapsed, average, or peak number of bytes processed by the device, board, or port during the user-defined time interval.

Setting the Timer Statistics Interval

To set the Timer Statistics time interval:

1. Click on the clock symbol (🕒) next to the **Interval** text box. The New Timer Interval text box, Figure 3-3, will appear.



00 : 00 : 30

Figure 3-3. New Timer Interval Text Box

2. Using the mouse, click to highlight the hour field in the New Timer Interval text box.
3. Using the arrow keys to the right of the text box, scroll to change the hour, as desired. Notice that the time is given in a 24-hour hh:mm:ss format.
4. Using steps 2 and 3, continue to change the minutes and seconds fields, as desired.
5. Click **OK** to accept your configurations, or click **Cancel** to exit the window without accepting any changes.

The Timer Statistics window will refresh to zero, and the new time interval will take effect immediately.

Summary Statistics

Using the Summary Statistics windows, you can graphically track the amount of activity (percent load, errors, and collisions) for which each board is responsible; you can also view board-level Summary Statistics, which display the amount of activity experienced by each port.

You can configure the Summary Statistics windows to view the percentage of the following network activity generated by devices attached to each board in your IRM2, and each port on a board:

- **Percent Load —** load generated, as a percentage of theoretical maximum load (10Mb / sec for Ethernet)

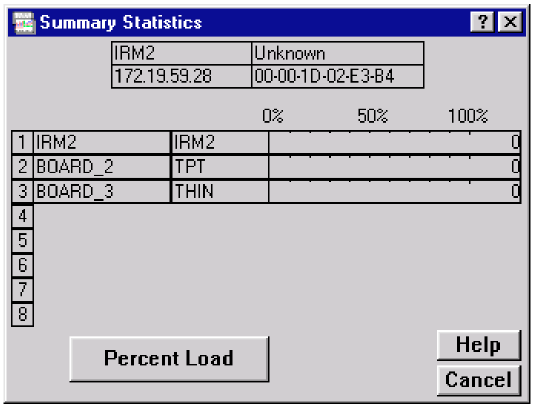
- **Percent Errors —** errors detected, as a percentage of total packets
- **Percent Collisions —** collisions detected, as a percentage of total packets

The dynamic bar graphs allow you to immediately observe the amount of activity experienced by each board or port; the scale displayed at the top right of the window indicates the percentage of activity represented by the bar.

Accessing the Summary Statistics Windows

To access the device-level Summary Statistics window:

1. Click on **Repeater** on the Chassis View menu bar to display the repeater menu.
2. Drag down to **Summary Statistics...** and release. The Repeater Summary Statistics window, Figure 3-4, will appear.



IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

1	IRM2	IRM2	0
2	BOARD_2	TPT	0
3	BOARD_3	THIN	0
4			
5			
6			
7			
8			

Figure 3-4. Device-level Summary Statistics Window

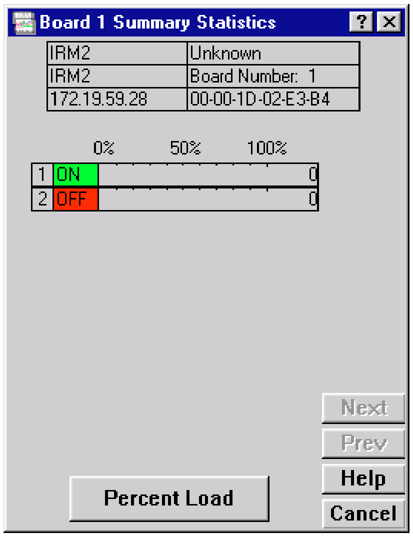
The device-level Summary Statistics window has three fields:

- The name assigned to each board (the number of the board indicates its position in the MMAC). The Summary Statistics window will always display 8 available slots; any slots not occupied by a board will remain empty.
- The type of board, such as **FOT** or **THN**.
- The Percent Load, Percent Errors, or Percent Collisions (indicated by the scale above the bar graph).

To open the board-level Summary Statistics window:

1. Click on the appropriate **Board number** in the Chassis View window to display the board menu.

2. Drag down to **Summary Statistics...** and release. The Board Summary Statistics window, Figure 3-5, will appear.



IRM2	Unknown
IRM2	Board Number: 1
172.19.59.28	00-00-1D-02-E3-B4

1	ON	0
2	OFF	0

Figure 3-5. Board-level Summary Statistics Window

The board-level Summary Statistics window also has three fields:

- The index number assigned to each port.
- The current status of the port: **ON**, **OFF**, **SEG**, or **NLK**. These status conditions and their associated colors are described in detail in Chapter 2 of this manual.
- The Percent Load, Percent Errors, or Percent Collisions (indicated by the scale above the bar graph).

NOTE

*If you are viewing a MIM with more than 12 ports, the **Prev** and **Next** buttons will be activated so that you can view all ports on the MIM.*

Configuring Summary Statistics

Both the device- and board-level Summary Statistics windows can be configured to display Percent Load, Percent Errors, or Percent Collisions.

To configure Summary Statistics:

1. Click **Percent Load**; a menu will appear.

2. Drag to select the desired mode: **Percent Load**, **Percent Errors**, or **Percent Collisions**. The button label will change to reflect the new mode, and the bar graph will refresh to display the current value.

Performance Graph

With the Repeater Performance Graphs, you can use real-time statistics reporting to see at a glance the amount of traffic going through your IRM2 at the repeater, board, or port level. The graph has an X axis that indicates the 60 second interval over which charting occurs continuously, while the Y axis measures the number of packets or errors that are processed by the device as a whole or by the selected board, or port.

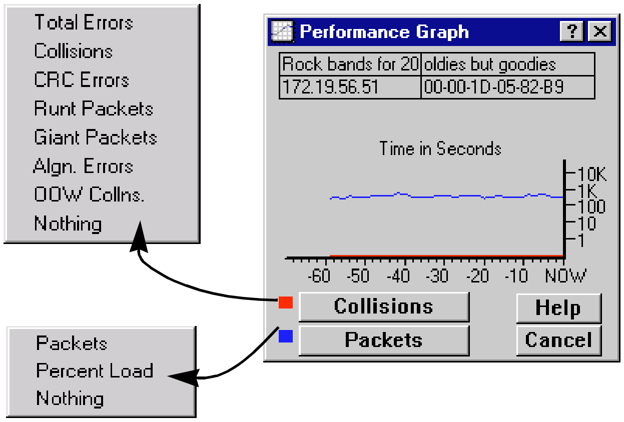
You can select the statistics that you wish to monitor by clicking the buttons at the lower left of the Performance Graph window. When clicked, each button displays a list of options; when you alter a parameter, the new parameter will appear on the face of the button, and the statistics will refresh to zero activity before regenerating.

Accessing the Performance Graph Windows

To access the Repeater Performance Graph window:

1. Click on **Repeater** on the Chassis View menu bar to display the repeater menu.

2. Drag down to **Performance Graph...** and release. The Repeater Performance Graphs window, Figure 3-6, will appear.



Rock bands for 20 | oldies but goodies
172.19.56.51 | 00-00-1D-05-82-B9

Figure 3-6. Performance Graph

To open the board-level Performance Graph window:

1. Click on the appropriate **Board number** to display the board menu.
2. Drag down to **Performance Graph...** and release. The board-level Performance Graph window will appear.

To access the port-level Performance Graph window:

1. Click on the appropriate **Port** to display the port menu.
2. Drag down to **Performance Graph...** and release. The port-level Performance Graph window will appear.

The Board and Port Performance Graph windows are the same as the Performance Graph window displayed in Figure 3-6, except that they display statistics applicable to the selected board or port. Each Performance Graph window allows you to graph the following statistical variables:

Total Errors

Total Errors

The total number of errors of any kind processed by the device, board, or port.

Collisions

The total number of collisions detected by the device, board, or port.

CRC Errors

The total number of packets with CRC (**C**yclical **R**edundancy **C**heck) detected by the device, board, or port.

Runt Packets

The number of runt packets detected by the device, board, or port. A runt frame is one that is less than the minimum Ethernet frame size of 64 bytes.

Giant Packets

The number of giant packets detected by the device, board, or port. A giant frame exceeds the maximum Ethernet frame size of 1518 bytes (excluding the preamble).

Algn. Errors

The number of misaligned packets detected by the device, board, or port. Misaligned packets are those which contain a non-integral number of bytes (that is, any unit of bits less than a byte); they can result from a MAC layer packet formation problem, or from a cabling problem that is corrupting or losing data.

OOW Collns.

The number of collisions out of the standard collision window (51.2 μs) detected by the device, board, or port. There are two conditions which can cause this type of error to occur: either the network's physical length exceeds IEEE 802.3 specifications, or a node on the net is transmitting without first listening for carrier sense (and beginning its illegal transmission more than 51.2 µs after the first station began transmitting).

Nothing — The Errors scale is not currently measuring any type of error packets.

Packets

Packets — The total number of good packets detected by the device, board, or port. Remember, this packet count does *not* include error packets.

Percent Load — Reflects the network load generated by the device, board, or port, compared to the theoretical maximum load (10Mbits/s) of an Ethernet network.

Nothing — The Packets scale is not currently measuring the number of packets coming through the device, board, or port.

Configuring the Performance Graph

To configure the Performance Graphs:

1. Click on **Collisions** to display the error mode menu.
2. Drag to select the desired errors mode. The error mode you have chosen will appear on the face of the button; the Performance Graph will refresh to zero and begin to measure using the new mode.
3. Click on **Packets** to display the packet mode menu.
4. Drag to select the desired packets mode. The packets mode you have chosen will appear on the face of the button; the Performance Graph will refresh to zero and begin to measure using the new mode.

The Performance Graph will now monitor the traffic passing through your IRM2 as a whole or the selected board or port using the user-defined modes. To stop monitoring and to exit the window, click Cancel.

Chapter 4

Source Address Functions

Using the Find Source Address window; locking and unlocking ports; viewing the source address table; setting the Device Ageing Time

Each Cabletron repeater device maintains a Source Address List, or Table (SAT), for each port. This table contains the MAC address for each device that is communicating through that port on the IRM2-controlled hub. Your Enterasys management application has three windows that allow you to use the IRM2 Source Addressing feature:

Find Source Address allows you to detect the specific IRM2 port through which a given MAC address is communicating.

Port Locking/Unlocking lets you secure your IRM2 against unknown source addresses trying to access a port.

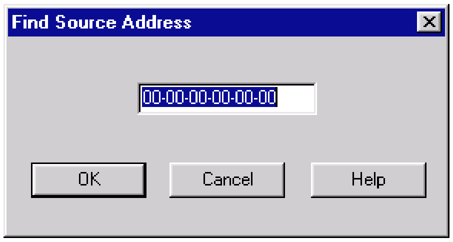
Source Addressing displays the source address table, which allows you to see the MAC address of each device communicating through a port.

Find Source Address

Find Source Address allows you to discover the port through which a specific Ethernet address is communicating.

To open the Find Source Address window:

1. Click on **Repeater** on the Chassis View menu bar.
2. Drag down to **Find Source Address...** and release. The Find Source Address window, Figure 4-1, will appear.



Find Source Address

00-00-00-00-00-00

Figure 4-1. Find Source Address Window

3. Enter the Ethernet address you wish to find in a hex XX-XX-XX-XX-XX-XX format in the text box.

4. Click OK; if you entered the MAC address incorrectly, a window will appear indicating that you entered an invalid address.

Enterasys' management application will check the device's database of source addresses; if the address is found, the port associated with the address will begin to flash. If the address is not found, a window will appear indicating that fact.

Using Port Locking and Unlocking

The Port Locking feature enables the IRM2 to prevent any new source addresses from accessing the ports connected to the repeater network. When a source address attempts to access a port, the IRM2 will compare that address to those in the Source Address Database for that port. For a **station port** (one detecting zero or one source addresses at the time locking was enabled), if the address is not found in the table, that port will automatically shut down, no traffic will be allowed through (although other station and trunk ports remain open), and a trap will be sent to the management station (if traps have been enabled). Note that the Device Ageing Time does ***not*** apply to station ports when Source Address Locking is enabled, although the snapshot of the Source Address Database provided by the Source Addressing window may show the detected source address ageing out if that address remains inactive, and the appropriate trap will be generated; see **Using Source Addressing**, page 4-4, for more information.

For a **trunk port** (one detecting two or more source addresses at the time locking was enabled) there is no port shut-down security feature; if port locking is enabled, all packets will continue to be allowed to pass.

NOTE

Note that when port locking is enabled, each port's topology status (trunk or station) remains fixed and will not change while locking remains enabled, regardless of any changes in the number of source addresses detected.

There are two ways to determine whether a port’s topology status is currently station or trunk:

1. Bring up that port’s Statistics window, and check the Active Users field. If Active Users is zero or one, the port is in station status; if it is two or more, the port is in trunk status.

   or

   Step 1. Bring up that port’s Source Addressing window; if zero or one source addresses appear, the port is in station status; if two or more appear, the port is in trunk status.

NOTE

A port in station status may actually be connected to multiple devices; station status simply indicates that no more than one device is currently active.

CAUTION

Use caution when implementing the Port Locking/Unlocking feature, particularly if all active ports are serving as station ports; it is conceivable that all station ports could be locked down, preventing any access to the device.

To use Port Locking:

1. Click on **Repeater** on the Chassis View menu bar. The repeater menu will appear.
2. Drag down to **Lock/Unlock Ports...** and release. The Lock/Unlock Ports window, Figure 4-2, will appear.

Figure 4-2. Lock / Unlock Ports Window

3. If the repeater’s ports are already locked, the window will note that they are locked, and ask if you want to unlock them; if they are not locked, the window will read as in Figure 4-2.
4. Click on the appropriate **Yes** or **No** button to lock or unlock the ports as desired.

NOTE

You must have superuser (SU) privileges to lock or unlock ports; i.e., the community name entered in the device's Describe window must provide SU access to the device.

When port locking is enabled, the Locked icon (🔒) will display in the Chassis View window. When Port Locking is disabled, the Unlocked icon (🔓) will display in the Chassis View window. As new source addresses attempt to access station ports, the port text boxes will turn red and display the word OFF, and the ports will be locked so that no traffic gets through — not even traffic from known source addresses. Once a port has been shut down because a new source address attempted access, it must be manually re-enabled using the **Enable** option on the appropriate Board or Port menu.

NOTE

On some older devices (or devices running older versions of firmware), unlinked ports will be disabled immediately after locking has been enabled; these ports can be re-enabled using their port menus, but they will immediately be disabled again if a device is connected and begins transmitting (since the port's source address table was locked in an empty state).

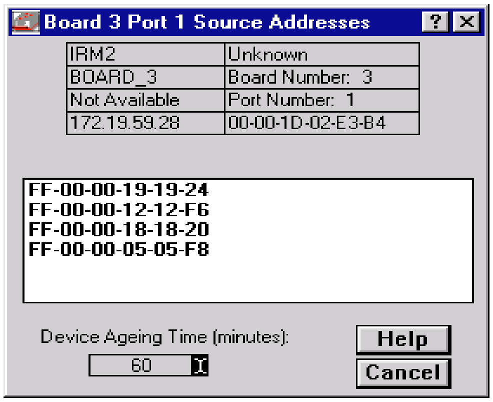
On devices with newer firmware, unlinked ports are not automatically disabled in response to port locking, but they, too, will be immediately disabled if a device is connected and attempts to transmit packets.

Using Source Addressing

Source Addressing allows you to display each port's Source Address Table, which lists the MAC addresses that are communicating through the selected port.

To open the Source Addresses window from the Chassis View:

1. Click on the appropriate port to display the Port menu.
2. Drag down to **Source Addressing...** and release. The Port Source Addresses window, Figure 4-3, will appear.



IRM2	Unknown
BOARD_3	Board Number: 3
Not Available	Port Number: 1
172.19.59.28	00-00-1D-02-E3-B4

FF-00-00-19-19-24
FF-00-00-12-12-F6
FF-00-00-18-18-20
FF-00-00-05-05-F8

Device Ageing Time (minutes): 60

Figure 4-3. Port Source Addresses Window

The source address list window displays the MAC addresses of all devices that have transmitted packets through the selected port within a time period less than the SAT's defined ageing time (addresses that have not transmitted a packet during one complete cycle of the ageing timer are purged). The Ageing Time is user-configurable; see **Setting the Device Ageing Time**, page 4-5.

NOTE

You can create a text file which will add names to correspond to the source addresses that appear in the Source Addresses window. For more information on how this naming feature works, refer to the ***NetSight Element Manager User's Guide.***

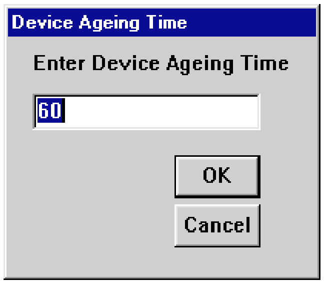
Setting the Device Ageing Time

The source address list Ageing Time determines the *minimum* amount of time an inactive source address will remain in the Source Address Table before it is purged. The source address timer runs continuously beginning at the time the device is turned on (or the repeater channel is activated); source addresses that are added to the SAT during one timer cycle will remain in the table for the rest of the current cycle, and at least through the next complete cycle. If no packets have been received from that address during one complete cycle, the address will be purged from the table.

The Ageing Time is user-configurable, and can be set using the Device Ageing Time window.

To set the Ageing Time:

1. Click the **I-bar cursor** (I) next to the Device Ageing Time field. The Device Ageing Time window, Figure 4-4, will appear.



Device Ageing Time

Enter Device Ageing Time

60

Figure 4-4. Device Ageing Time Window

2. Enter the new Ageing Time in minutes. Allowable times are **1** to **1440**.

3. Click OK to accept the new Ageing Time, or click **Cancel** to exit the window without making any changes.

Chapter 5

Alarm Limits

Accessing the repeater, board, and port Alarm Limits windows; setting alarm limits based on percentage of collisions, packet count, broadcast packet count, or percentage of errors; setting the alarm limits time interval; using the Disable Board/Disable Port on Alarm option

Using the Alarm Limits windows, you can configure alarm limits for the IRM2 at the repeater, board, and port levels; these alarms will notify you — via traps sent to your Enterasys management application's alarm logging facility — that your system has experienced a certain percentage of collisions or errors, or a certain number of specific packet types, within a user-defined time interval. You can also use the board- and port-level Alarms windows to disable a board or port in response to an alarm condition.

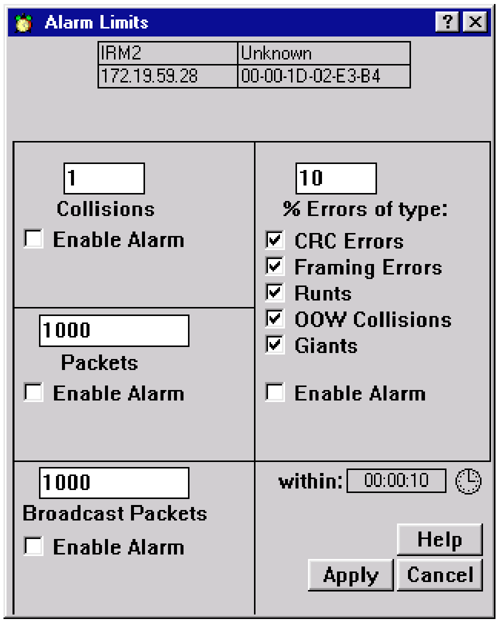
NOTE

In order for your device to issue any traps — and in order for your management workstation to receive those traps — your IRM2's trap table must have been properly configured via Local Management; see the IRM2 hardware manual for more information.

Accessing the Alarm Limits Windows

To open the repeater-level Alarm Limits window from the Chassis View:

1. Click on **Repeater** on the Chassis View menu bar to reveal the Repeater menu.
2. Drag down to **Alarm Limits...** and release. The Repeater Alarm Limits window, Figure 5-1, will appear.



IRM2	Unknown
172.19.59.28	00-00-1D-02-E3-B4

1 Collisions
☐ Enable Alarm

1000 Packets
☐ Enable Alarm

1000 Broadcast Packets
☐ Enable Alarm

10 % Errors of type:
☑ CRC Errors
☑ Framing Errors
☑ Runts
☑ OOW Collisions
☑ Giants

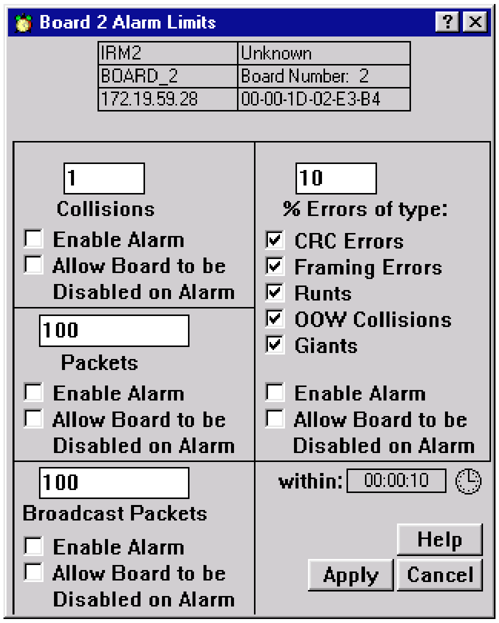
☐ Enable Alarm

within: 00:00:10

Figure 5-1. Repeater Alarm Limits Window

To access the board-level Alarm Limits window:

1. Click once on the appropriate **Board number** in the Chassis View to display the board menu will appear.
2. Drag down to **Alarm Limits...** and release. The Board Alarm Limits window, Figure 5-2, will appear.



Board 2 Alarm Limits

IRM2	Unknown
BOARD_2	Board Number: 2
172.19.59.28	00-00-1D-02-E3-B4

1
Collisions
□ Enable Alarm
□ Allow Board to be Disabled on Alarm

100
Packets
□ Enable Alarm
□ Allow Board to be Disabled on Alarm

100
Broadcast Packets
□ Enable Alarm
□ Allow Board to be Disabled on Alarm

10
% Errors of type:
☑ CRC Errors
☑ Framing Errors
☑ Runts
☑ OOW Collisions
☑ Giants

□ Enable Alarm
□ Allow Board to be Disabled on Alarm

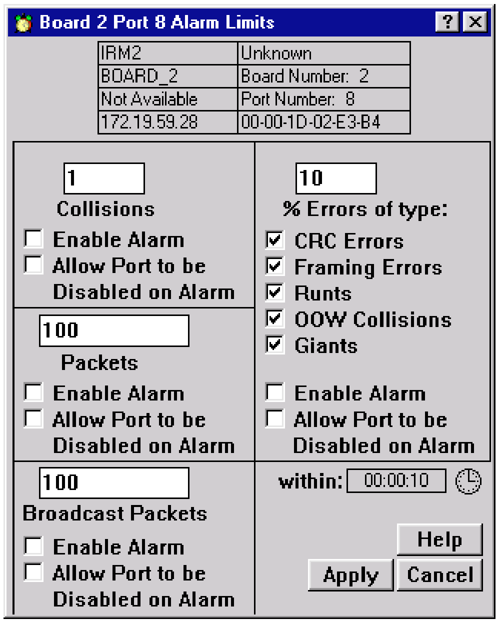
within: 00:00:10

Figure 5-2. Board Alarm Limits Window

To access the port-level Alarm Limits window:

1. Click once on the appropriate **Port** to display the port menu.
2. Drag down to **Alarm Limits...** and release. The Port Alarm Limits window, Figure 5-3, will appear.

.



Board 2 Port 8 Alarm Limits

IRM2	Unknown
BOARD_2	Board Number: 2
Not Available	Port Number: 8
172.19.59.28	00-00-1D-02-E3-B4

1 Collisions
□ Enable Alarm
□ Allow Port to be Disabled on Alarm

100 Packets
□ Enable Alarm
□ Allow Port to be Disabled on Alarm

100 Broadcast Packets
□ Enable Alarm
□ Allow Port to be Disabled on Alarm

10 % Errors of type:
☑ CRC Errors
☑ Framing Errors
☑ Runts
☑ OOW Collisions
☑ Giants

□ Enable Alarm
□ Allow Port to be Disabled on Alarm

within: 00:00:10

Figure 5-3. Port Alarm Limits Window

When using the Alarm Limits screens to set your alarm thresholds, keep in mind that repeater-level thresholds will apply to all traffic received by the entire IRM2-managed repeater segment; board-level thresholds will apply only to traffic on the selected board; and port-level thresholds will apply to traffic on the specific port.

The Alarm Limits window displays the following fields:

NOTE

Some IRM2s running older revisions of firmware (version 1.0) will not support all of the alarm fields described below; any fields which appear grayed out are not supported by the modeled device.

Collisions

Use the text box in this field to enter the number of collisions per good packet you wish to allow on the selected repeater, board, or port before an alarm is generated; allowable values are 1-15. For example, if you enter a value of 1, the alarm will be generated if the repeater, board, or port experiences an average of one collision per good packet received during the configured time base (see the explanation for “within,” below). In terms of percentages, an alarm threshold value of 1 would generate an alarm if 50% of your packets were collisions (one collision for every good packet); a threshold value of 15 would generate an alarm if 93.75% of your packets were collisions (15 collisions for every good packet). Therefore, the lower you set your threshold value, the lower the percentage of collisions per good packet you are allowing.

Remember, a repeater-level alarm will calculate the number of collisions per good packet based on all traffic received on the repeater channel; a board- or port-level alarm will make the calculation based on traffic on the specific board or port only.

Packets

Use the text box in this field to determine the number of good packets (excluding all errors) that must be processed by the repeater, board, or port within the user-specified time before an alarm is triggered. Allowable values are 1 to Ý 4 billion (2^{32}-1).

Broadcast Packets

Use the text box in this field to determine the number of broadcast packets that must be processed by the repeater, board, or port within the user-specified time before an alarm limit is reached. Allowable values are 1 to Ý 4 billion (2^{32}-1).

% Errors of Type

Use the text box in this field to determine what percentage of packets received by the repeater, board, or port within the specified time interval can be errors of the selected type or types before an alarm is triggered. Allowable values are 1 to 100; percentages will be calculated based on the number of error packets of all types selected (all those with an X in their check box). Again, a repeater-level alarm will count all selected error types received by the repeater; a board- or port-level alarm will count all selected error types received by the individual board or port.

You can select any combination of the following error types:

CRC Errors

If this check box is selected, all packets with Cyclical Redundancy Check (CRC) errors will be included in calculating the overall percentage of errors.

Framing Errors

If this check box is selected, all misaligned packets will be included in calculating the overall percentage of errors. A misaligned packet is one with a non-integral number of bytes; these are also sometimes referred to as alignment errors.

Runts

If this check box is selected, the number of runt packets will be included in calculating the overall percentage of errors. A runt packet is one that is less than the minimum Ethernet frame size of 64 bytes.

OOW Collisions

If this check box is selected, all collisions out of the standard collision window (51.2 µs) will be included in calculating the overall percentage of errors. Out-of-window collisions are typically caused by faulty network design.

Giants

If this check box is selected, the number of giant packets will be included in calculating the overall percentage of errors. A giant packet exceeds the maximum Ethernet frame size of 1518 bytes (excluding the preamble).

within:

This field displays the user-configurable alarm limit timer interval: the amount of time the selected statistics will be counted before being compared to the configured thresholds. The allowable values are 10 seconds to 23 hours / 59 minutes / 59 seconds.

Configuring Alarms

You configure alarms by choosing the alarm you wish to enable, setting the threshold to the desired level, and selecting a time interval within which that threshold must occur. You can base the alarms on:

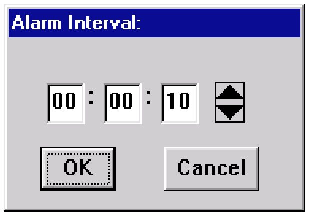
- Number of collisions per good packet
- Number of total packets
- Number of broadcast packets
- Percentage of error packets

You can also configure board or port alarm limits so that the board or port will be disabled when an alarm limit is reached.

Setting the Alarm Limits Time Interval

To set the time interval within which the defined alarm thresholds must be reached in order to trigger an alarm:

1. Click on the clock 🕓 next to the **within:** text box in any one of the alarm limits windows; the interval you set applies to all configured alarms at all levels. The Alarm Interval window, Figure 5-4, will appear.



Alarm Interval:

00 : 00 : 10

Figure 5-4. Alarm Interval Window

2. Highlight the **hour** text box (the first box to the left).
3. Click on the up and down arrows to change the time, or type in the new hour time interval.
4. Repeat steps 2 and 3 to set the minutes and seconds of your new time interval. Remember, the maximum time setting is 23 hrs/59 minutes/59 seconds.
5. Click on OK . The new Alarm Interval you have set will appear in the **within:** text box.
6. Click on Set at the bottom of the Alarm Limits window to save your changes, then click on **Cancel** to close the window. Be sure to click on Set before closing the window, or your changes will not be saved.

Setting Alarm Limits

To set repeater-, board-, or port-level alarms, first be sure you have opened the appropriate Alarm Limits window, then follow the steps outlined below:

1. Using the mouse, click and drag to highlight the text box in the alarm field you wish to configure (**Collisions**, **Packets**, **Broadcast Packets**, or **% Errors of Type**).
2. Enter the desired threshold value, being sure to keep in mind the units and range limits described above.
3. Click on the **Enable Alarm** check box to activate it. (A check box is activated if there is an X in it.)
4. For board- or port-level alarms only, click on the **Allow Board/Port to be Disabled on Alarm** check box if you wish to disable the board or port when an alarm condition occurs.

NOTE

*If you activate the **Allow Board/Port to be Disabled on Alarm** option, you will have to manually re-enable the board(s) or port(s) if the alarm is triggered. Resetting the device will clear the condition by clearing all packet counters, but you will still need to re-enable the board(s) and/or port(s).*

5. Repeat steps 1-4 for each type of alarm you wish to configure.
6. Click on Set to save the configuration, then click **Cancel** to close the window. Be sure to click on Set before closing the window, or your changes will not be saved.

Your Alarm Limits are now set. Any condition that exceeds these alarm limits will generate an alarm, and disable that board or port, if so configured.

Refer to your ***Enterasys'Alarm and Event Handling User's Guide*** for information on how to use its alarm logging facilities to view alarms.

Trap Selection

Accessing the Trap Selection window; link state traps, segmentation traps, and source address traps defined; enabling and disabling traps

Among the traps which Enterasys and Cabletron devices are designed to generate are traps which indicate when a repeater port gains or loses a link signal (Link State Traps); when the repeater segments (disconnects) a port due to collision activity, and when a segmented port becomes active again (Segmentation Traps); and several traps that result from changes in a port's Source Address Table (Source Address Traps). In some networks, these traps may be more information than a network manager wants to see. With the Trap Selection option available from the Repeater menu, you can enable or disable these traps at all ports on the device.

Any traps issued by the IRM2 will appear in your Enterasys remote management application's alarm logging facility. (Refer to your ***Alarm and Event Handling User's Guide*** for more details.)

NOTE

In order for your device to issue any traps — and in order for your management workstation to receive those traps — your IRM2's trap table must have been properly configured via Local Management; see the IRM2 hardware manual or Local Management documentation for more information.

Note also that some older Enterasys and Cabletron devices and/or firmware versions, including the IRM2, do not support Source Address traps.

Accessing the Trap Selection Windows

To open the repeater-level Trap Selection window from the Chassis View:

1. Click on **Repeater** on the Chassis View menu bar, drag down to the appropriate repeater selection, then right to reveal the Repeater menu.

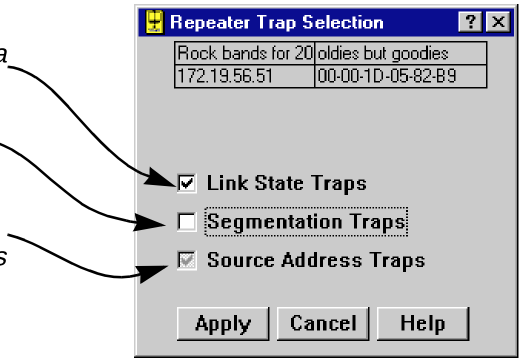
2. Drag down to **Trap Selection...** and release. The Repeater Trap Selection window, Figure 6-1, will appear.

At the repeater level, a check box indicates the state of settings for all ports that are on the device. The check box will be:

Checked — If all port trap settings are enabled for a given trap.

Blank — if all port trap settings are disabled for a given trap.

A Gray check box will also appear as you toggle a trap between the enabled and disabled states. This gray box simply serves to indicate a “No Change” for the value. Leaving a trap state at its original value OR leaving the gray “No Change” state will both have the same effect; namely leaving the current state set for the trap.



Repeater Trap Selection

Rock bands for 20	oldies but goodies
172.19.56.51	00-00-1D-05-82-B9

☑ Link State Traps

□ Segmentation Traps

☑ Source Address Traps

Figure 6-1. Repeater Trap Selection Window

Trap Definitions

You can enable or disable the following kinds of traps:

Link State Traps

Some Enterasys and Cabletron Ethernet repeater ports — including RJ45 twisted pair and fiber optic ports — generate a link signal to monitor the status of their connection with the device at the other end of the cable segment. If the cable is removed or broken, the port’s link status goes to “No Link” and the repeater generates a **portLinkDown** trap. When a port in a “No Link” condition receives a link signal, the port goes to a “Link” condition and the repeater generates a **portLinkUp** trap. Devices at both ends of the disconnected or broken cable will generate the **portLinkDown** and **portLinkUp** traps, even when only one end of the cable has been removed.

Note that BNC (thin coax), AUI, and transceiver ports do not support a link signal. BNC ports respond to changes in link status by generating **portSegmenting** and **portUnsegmenting** traps (see description, below); AUI and transceiver ports do not respond at all to changes in link status (unless the port has been segmented due to excessive collisions), and will always display as on, even if no cable is connected.

Information included in a Link State trap will include the hub number and port number associated with the trap.

Segmentation Traps

Enterasys' and Cabletron's Ethernet repeaters count collisions at each port. If a port experiences 32 consecutive collisions, or if the port's collision detector is on for more than

2-3 µs, the repeater segments the port to isolate the source of the collisions from the rest of the network. When the repeater segments a port, it generates a **portSegmenting** trap. As soon as a segmented port receives a good packet, the repeater reconnects the port to the network and generates a **portUnsegmenting** trap.

Note that, because they do not support the Link signal, unterminated BNC (thin coax) ports appear as segmented. When you attach a thin coax cable or a terminator to a port, the repeater generates a **portUnsegmenting** trap; when you remove the cable or terminator, the repeater generates a **portSegmenting trap**. As mentioned above, these traps can serve as notification of changes in link status. Note, too, that devices at both ends of the cable segment will generate the **portSegmenting** and **portUnsegmenting** traps, even if only one end of the cable has been disconnected.

Information included in a Segmentation trap will include the hub number and port number associated with the trap.

Source Address Traps

The IRM2 can issue several different traps in response to changes in a port's Source Address Table:

A **newSourceAddress** trap is generated when a station port — one receiving packets from no source addresses, or from a single source address — receives a packet from a source address that is not currently in its source address table. Information included in this trap includes the hub number, port number, and source address associated with the trap. Trunk ports — those receiving packets from two or more source addresses — will not issue new Source Address traps.

A **sourceAddressTimeout** trap is issued anytime a source address is aged out of the Source Address Table due to inactivity. The trap's interesting information includes the hub and port index, and the source address that timed out. (See Chapter 4, **Source Address Functions**, for more information on the ageing time.)

PortTypeChanged traps are issued when a port's topology status changes from station to trunk, or vice versa. The interesting information includes the hub and port index, and the port's new topology status.

A **lockStatusChanged** trap is generated when the ports in the hub are locked or unlocked using the Lock/Unlock Ports option on the Repeater menus; the interesting information is the new lock status. (See **Lock/Unlock Ports** in Chapter 4 for more information.)

PortSecurityViolation and **portViolationReset** traps are sent in response to changes related to port locking: if ports are locked, the **portSecurityViolation** trap indicates that a new source address has attempted access on one of the ports, and the ports are being shut down in response; the interesting information is the hub and port index, and the violating address. **PortViolationReset** traps are sent when management intervention has re-enabled a port or ports previously disabled in response to a port security violation; the interesting information is hub and port index. Again, see **Lock/Unlock Ports** in Chapter 4 for more information.

Configuring Traps

The current status (enabled or disabled) for Link State, Segmentation, and Source Address traps will always be displayed when you first the port-level Trap Selection window.

When you are changing trap settings at the Repeater level, a check box that is toggled to gray for a given trap is treated as a "No SET" indicator, so that the current settings for all ports with respect to that trap will *not* be overridden when you are changing other trap settings. The gray mode will never appear when you first open the window (since a given trap can only be enabled or disabled for all ports on the device). Although you can change a check box to gray to indicate a "No SET" state, there is no practical reason to do so.

To enable or disable the above-described traps at all ports on your IRM2:

1. Open the Repeater Trap Selection window.
2. Click on the **check box** next to the desired trap: Link State, Segmentation, or Source Address.
   - An empty check box indicates that the corresponding trap is **disabled**;
   - A check box with an **X** indicates that the corresponding trap is **enabled**;
   - A check box that remains gray indicates that the associated trap will *not* be set (to either enabled or disabled), and the currently set mode will be maintained.
3. Click on **Apply**. The device will now issue, or stop issuing, the indicated traps to your management workstation. Keep in mind, however, that no traps will be issued to your management station unless the IRM2's trap table has been properly configured via Local Management! Consult your IRM2 Local Management documentation for more information.
4. Click on **Cancel** to exit the window; note that clicking on **Cancel** before clicking on **Apply** will close the window without making any changes.

Chapter 7

Redundancy

Accessing the redundancy window; establishing a redundant circuit; activating the circuit; testing the circuits; reconfiguring a circuit; changing port status; resetting a circuit

The redundancy application allows you to establish redundant circuits on the IRM2's repeater segment to ensure that vital network connections do not fail. Once configured and enabled, a redundant circuit ensures that, in addition to a primary network link to a port in the IRM2 managed-hub, there are several backup links that will automatically assume operation should the primary (or subsequent backup) link fail.

The IRM2 monitors the link status of the primary port for each redundant circuit by polling the physical addresses of designated nodes on the circuit using an Enterasys proprietary poll. Should all addresses fail to respond to the poll, a backup link will take effect. This reduces the risk of total network failure because of one faulty link.

CAUTION

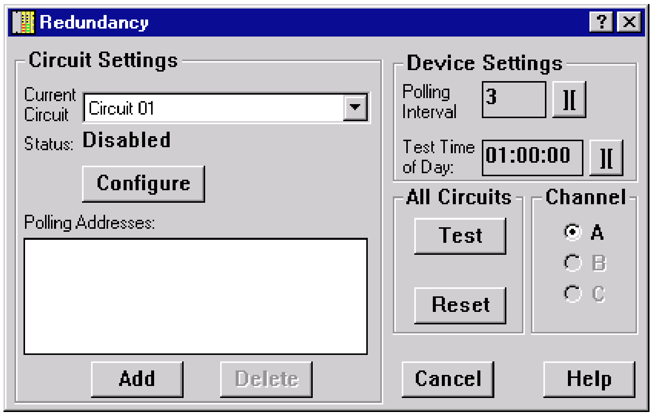
Before you configure redundancy, make sure that only the primary links are physically connected to the network. If you have all your backup ports physically connected before redundancy is configured ***and enabled****, you will create multiple data loops on your network.*

Accessing the Redundancy Window

To open the Redundancy window:

1. Click on **View** on the Chassis View menu bar.
2. Drag down to **Redundancy**, and release.

Two things will occur when you select the Redundancy View: the Redundancy Configuration window, Figure 7-1, will appear; and the Chassis View will change significantly, as illustrated in Figure 7-2. You will use these two windows in tandem to configure your redundant circuits.



Current Circuit: Circuit 01

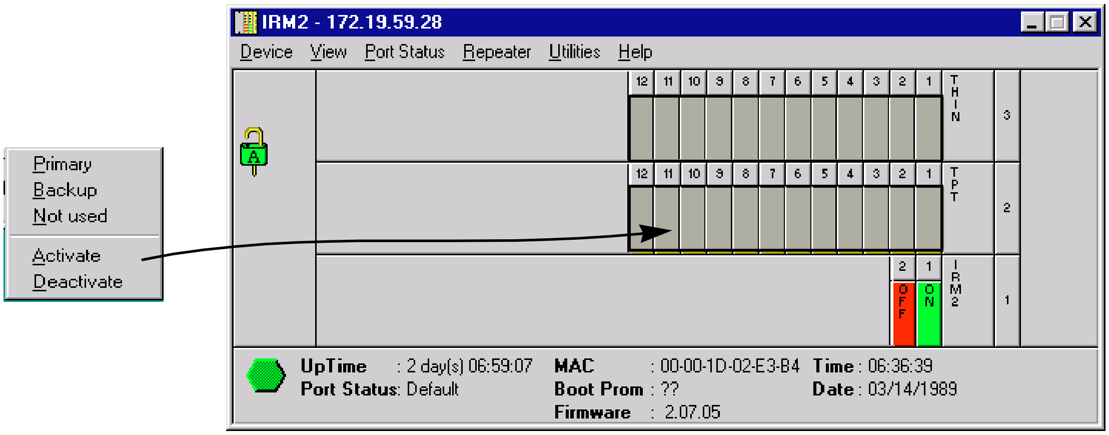
Status: Disabled

Polling Interval: 3

Test Time of Day: 01:00:00

Channel: ● A ○ B ○ C

Figure 7-1. Redundancy Configuration Window



UpTime : 2 day(s) 06:59:07
Port Status: Default
MAC : 00-00-1D-02-E3-B4
Boot Prom : ??
Firmware : 2.07.05
Time : 06:36:39
Date : 03/14/1989

Figure 7-2. Chassis View in Redundancy Mode

The Redundancy Configuration window, Figure 7-1, allows you to add or delete a redundant circuit for your IRM2, as well as Rename, Reset, Enable, Disable, or reconfigure the Retry Count for any circuits you have configured.

The altered Chassis View display, Figure 7-2, provides the means by which you assign primary and backup ports to each circuit.

Establishing Redundancy

You establish redundancy for the selected IRM2 by:

- Ensuring that, until redundancy is configured and enabled, only the primary links are physically connected to the network. If you have all your backup ports physically connected before your redundant circuits are configured and enabled, you will create multiple data loops on your network
- Selecting one of the available redundant circuits; each circuit ensures that a vital network connection remains active
- Entering the physical addresses of the intelligent Enterasys and Cabletron devices that will be polled to test the link associated with the circuit and verify that it is still operational
- Specifying all ports on the selected IRM2 that will act as network links for the circuit
- Assigning a priority to each port (primary or backup)
- Enabling the circuit
- Physically connecting the backup ports **after** completely configuring and enabling the circuit

After setting up the redundancy scheme for the selected IRM2, you can establish the testing interval that confirms that all circuits are operational. You can also reconfigure your circuits, if desired.

Selecting and Naming a Circuit

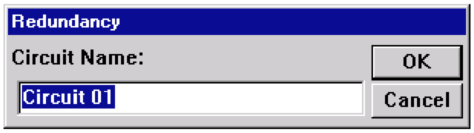
The first step in configuring a redundant circuit is to select, and, if you wish, name the circuit that you want to configure.

To select a circuit:

1. Click on the arrow to the right of the Current Circuit text box, and scroll through the Circuit list to select the desired circuit. The IRM2 supports up to sixteen circuits; you cannot add additional circuits to the list.
2. Click on the desired circuit number or name. The circuit will be highlighted and displayed in the Current Circuit text box to show that it has been selected.

To name a circuit:

1. With the circuit you have selected still highlighted, click **Configure**.
2. Drag down to **Rename**, and release. The Circuit Name window, Figure 7-3, will appear.



Circuit Name: Circuit 01

Figure 7-3. Circuit Name Window

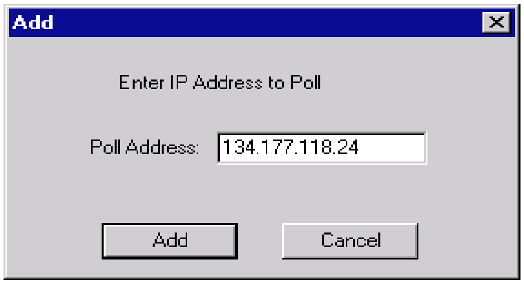
3. Enter your new name in the text field, and click **OK**. The new name will appear in the Current Circuit text box. To exit the window without accepting any changes, click **Cancel**.

Entering the Physical Addresses of Devices to be Polled

You must designate the physical address of at least one intelligent Enterasys or Cabletron device on your network to poll; the maximum number of addresses per circuit is eight. These addresses define the destination nodes your Enterasys management application will look for to determine the status of the active link. The IRM2 will simultaneously poll all addresses on each circuit's list; if it cannot establish a link with any address on the list after the designated number of retries, the IRM2 assumes the circuit is down and switches traffic to a designated backup port.

To designate the polling addresses for a circuit:

1. With the selected circuit still displayed in the Current Circuit box, click on **Add**; the Add Poll Address window, Figure 7-4, will appear.



Poll Address: 134.177.118.24

Figure 7-4. Add Polling Address Window

2. Enter the physical address of the device you want polled.

3. Click **Add** to add the address to the list. If you have entered an address that is not in the correct XX-XX-XX-XX-XX-XX hexadecimal format, an error message will appear, and no address will be added to the list.

Repeat steps 1-3 to designate all devices you wish to poll to test that the current link is active, up to the maximum number permitted by your device's firmware.

4. To delete an address that has already been added to the list, highlight the entry and click on **Delete**; the address will be removed from the list.

Assigning Backup Ports and Port Priority to the Circuit

Each circuit contains one primary port and several additional ports that serve as backups. If the primary port fails, the redundancy path will switch to the **first** backup port specified, and as necessary, switch to subsequent backup ports in the order in which they were specified. The maximum number of ports that can be configured for a circuit is eight.

As noted above, you will use the altered Chassis View display to assign ports to your redundant circuit. The port you designate as primary will turn green; the remaining backup ports will display in gray. Once redundancy is enabled, whichever port is the current active link in the redundant circuit will display in green.

To select the primary and backup paths for the designated circuit:

1. In the altered Chassis View window (Figure 7-2), click on the port that you wish to specify as primary. A port menu will appear.
2. Select **Primary**. The port will be designated as "**PRI**," and the port box will turn green.
3. Click on the port that you wish to specify as the first backup port. Again, the port menu will appear.
4. Select **Backup**. The port will be designated as "**BKP**," and will remain gray. Once the circuit is enabled, this and all backup ports will be disabled by management; backup ports will remain disabled until such time as they become active by virtue of primary port failure, or until they are manually re-enabled once the redundant circuit has been disabled.
5. To specify further backup ports, repeat steps 3 and 4. Be sure to specify each backup port in the order you wish it to assume redundancy.

The first port you specify will remain the default active link, even if you designate that port as a backup and designate a *different* port as primary. If you wish to ensure that the primary port will be the first active port in the circuit, you can use the **Activate** command from the port menu to override the firmware default. See **Changing Port Status**, page 7-10, for more information.

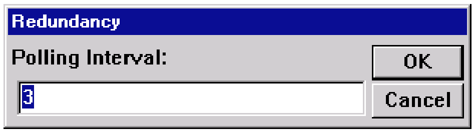
Setting the Polling Interval and Number of Retries

Once you have configured your redundant circuits, you can set the parameters that the IRM2 uses to monitor them, including the interval (in seconds) between polls of the physical addresses on your Polling Addresses list, and the number of times to retry polling for each circuit.

To test each enabled circuit, the IRM2 polls each address in the Polling Addresses list simultaneously, then waits the number of seconds set in the Polling Interval field for a reply. If at least one reply is received during the polling interval, the IRM2 simply polls all addresses again at the end of the interval. If no reply is received during the polling interval, the IRM2 will continue polling for the number of retries set for each circuit; if at least one reply is received during a retry, polling continues. If no replies are received during the retries, the IRM2 will assume the primary link is down, and switch traffic to the first backup port.

To establish the polling interval for all circuits:

1. Click on the gray button to the right of the Polling Interval field in the upper right-hand corner of the Redundancy Configuration window; the Polling Interval window, Figure 7-5, will appear.


Redundancy

Polling Interval: 3

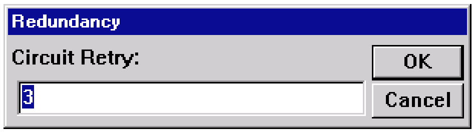
Figure 7-5. Polling Interval Window

2. Type in the number of seconds you want between polls to the network addresses listed for each enabled circuit. The range is 0–99 seconds; the default value is 3.

3. Click on OK to set the new polling interval, or on **Cancel** to close the window without making any changes. Note that the polling interval you set here will be applied to *all* active circuits; you cannot set individual polling intervals.

To establish the number of retries for the designated circuit:

1. Click on **Configure** to display the circuit configuration menu; drag down to **Retry Count**, and release. The Retry Count window, Figure 7-6, will appear.


Redundancy

Circuit Retry: 3

Figure 7-6. Retry Count Window

2. Enter the number of polls that must entirely fail before the redundant circuit switches to the next backup port, then click OK . The range is 1–16; the default value is 3. Note that the retry count you set here applies *only* to the currently selected circuit; you must specify a retry count for each individual circuit.

NOTE

If you are polling devices that are some distance from the IRM2, or if your network is somewhat slow, be sure to set your polling interval and/or number of retries accordingly to avoid the unnecessary use of backup ports.

If your primary port should fail and traffic is switched to a backup port, that backup port will remain the active port unless it, too, fails, or until the primary port is repaired and the circuits are tested. See **Testing the Circuits**, page 7-8, for more information.

Activating the Circuit

Once you have defined all port paths for a circuit, designated the device addresses to poll, and set the appropriate polling interval and number of retries, you can activate the circuit.

The activation criteria for a circuit are:

- You must have at least two ports associated with the circuit: one as Primary, and at least one as Backup
- You must have at least one address entered in the Polled Addresses list

To activate the circuit:

1. Use the drop-down list to display the appropriate circuit in the Current Circuit text box; note that the current status of the selected circuit (enabled or disabled) is displayed just below the Current Circuit text box.
2. Click **Configure**, and drag down to **Enable** to activate the currently selected circuit. The defined redundancy scheme for that circuit will take effect, and the displayed status for the selected circuit will change to **Enabled**.
3. Make all physical connections to your defined backup ports. Backup ports are automatically disabled by management once a redundant circuit has been enabled, and will not be re-enabled unless the primary port in the redundant circuit fails, or unless they are manually re-enabled once the redundant circuit has been disabled.

While redundancy is in effect, the Redundancy mode of the Chassis View window will display the current active port in green; backup ports and failed ports will both display in gray.

CAUTION *Be sure to physically connect your backup ports once your redundant circuit has been enabled!*

To disable a circuit:

1. Use the drop-down list to display the appropriate circuit in the Current Circuit text box; note that the current status of the selected circuit (enabled or disabled) is displayed just below the Current Circuit text box.
2. Click **Configure**, and drag down to **Disable** to inactivate the currently selected circuit. The displayed status for the selected circuit will change to **Disabled**.

CAUTION *If you do not plan to re-enable the circuit, remember that all configured backup ports will remain disabled by management until they are manually re-enabled using the port menus from the Chassis View window (in Logical display mode). If you do decide to re-enable your backup ports, be sure to disconnect redundant network links before doing so, or multiple data loops will result.*

Testing the Circuits

The circuit test checks the current status of every port link, both primary and backup, by polling the physical addresses in each circuit's Polling Addresses list through each port configured as part of the circuit. This test can be performed at a pre-determined time or date, or manually at any time.

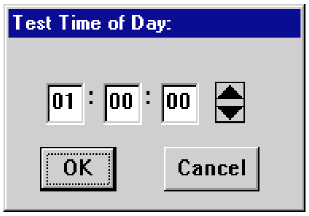
If the test detects any problems with the ports on a circuit, whether active or backup, it will list the circuit and its problem ports in the alarm logging facility. (Refer to the ***Alarm and Event Handling User's Guide f***or your Enterasys management application for more information.)

The testing begins at each circuit's currently active port; all ports are tested in sequence. Once testing is finished, the circuits will be reset so that the port designated as Primary will become the active port; if the primary port is not operational, the next operational backup port will be activated.

NOTE *A primary port that has failed, then been repaired, is not returned to active status until the circuit test is run, unless all other backup ports on the circuit have failed in the interim.*

To establish a daily time of day for a test:

1. In the upper right hand corner of the Redundancy Configuration window, click on the gray box to the right of the **Test Time of Day** text box. The Test Time of Day window, Figure 7-7, will appear.



01 : 00 : 00

Figure 7-7. Test Time of Day Window

2. Using the mouse, click to highlight the hour field in the New Timer Interval text box.
3. Using the arrow keys to the right of the text box, scroll to change the hour, as desired.
4. Using step 2 and 3, continue to change the minutes and seconds fields as desired (the default value is 1:00:00 a.m.).
5. Click OK to accept the new time, or click **Cancel** to exit the window without accepting any changes.

To perform an immediate test of all circuits:

1. Click **Test** in the Redundancy Configuration window. All configured circuits will be tested immediately.

Reconfiguring a Circuit

Once a circuit is enabled, the redundancy scheme will operate automatically. However, you may wish to alter its configuration after it is initially enabled. You can alter the **Circuit Name** or **Retry Count**, as described in previous sections, while a circuit is enabled. However, to change the port status or address information of an enabled circuit, you must first disable it.

To do so:

1. Use the drop-down list to display the appropriate circuit in the Current Circuit text box; note that the current status of the selected circuit (enabled or disabled) is displayed just below the Current Circuit text box.
2. Click **Configure**, and drag down to **Disable** to inactivate the currently selected circuit. The displayed status for the selected circuit will change to Disabled.

Redundancy will no longer be in effect for that circuit, and you can now reconfigure and re-enable it.

CAUTION

If you disable a circuit with no plans to re-enable it, remember that all configured backup ports will remain disabled by management until they are manually re-enabled using the port menus from the Chassis View window (in Logical display mode). If you do decide to re-enable your backup ports, be sure to disconnect redundant network links before doing so, or multiple data loops will result.

Changing Port Status

To specify a port as the current active link:

1. On the altered Chassis View, click on the port that you wish to specify as the active link port.
2. Select **Activate** to make the port the active link. The port will retain its originally defined priority (primary or backup), but will turn green to indicate that it is currently the active port.

The next Backup port will now be the one specified subsequently when the circuit was defined.

To deactivate a port from active link status to inactive status:

1. On the altered Chassis View, click on the port which is the current active link.
2. Select **Deactivate**. The port will retain its originally defined priority (primary or backup), but will revert to inactive status.

NOTE

If you deactivate the current active link, no other port in the circuit will automatically be activated; be sure to use the port menus to activate another port in the circuit, or you will not be allowed to re-enable the circuit.

To remove a port from a circuit:

1. On the altered Chassis View, click on the port that you wish to remove from the circuit.
2. Select **Not used** to remove the port from the circuit.

The port will now revert to its initial gray display, indicating that it is no longer connected with the circuit; if you have removed the current active link, the next port in the path will automatically be activated.

NOTE

Any backup port which has been part of an enabled circuit will remain disabled by management until you turn it back on at the Chassis View window (in Logical mode), so that accidental data loops do not occur. Be sure to disconnect any redundant network links before re-enabling ports.

To change a port's designation from primary to backup, or vice versa:

1. On the altered Chassis View, click on the port whose designation you wish to change.
2. Select **Primary** or **Backup**, as appropriate, to change the port's designation.

Note that changing a port's designation as primary or backup will not change its current active or inactive status; if you wish to activate a port you have just changed from backup to primary, or deactivate a port you have just changed from primary to backup, you must also use the **Activate** and **Deactivate** commands described above.

Resetting a Circuit

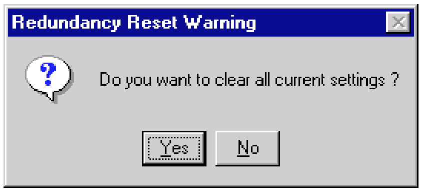
Resetting a circuit changes the status of the circuit to disabled, deletes all entries in the Polling Address list, and clears all port designations. You can reset circuits individually or collectively.

To reset an **individual** circuit:

1. Use the drop-down list to display the appropriate circuit in the Current Circuit text box; note that the current status of the selected circuit (enabled or disabled) is displayed just below the Current Circuit text box.
2. Click on **Configure**, and select **Reset**. This will clear all redundancy settings for the selected circuit, and restore it to its original undefined and disabled status.

To reset **all** circuits at once:

1. Click **Reset**. A warning window will appear (Figure 7-8), asking you to confirm your selection.



Do you want to clear all current settings ?

Figure 7-8. Redundancy Reset Warning Window

2. If you select **Yes**, all circuits will be reset to their initial default status, regardless of whether they are currently enabled or disabled. If you select **No**, circuits will remain in their current condition.

CAUTION

Any backup port which has been part of an enabled redundant circuit will remain disabled by management until you turn it back on at the Chassis View window (in Logical mode), so that accidental data loops do not occur. Be sure to disconnect any redundant network links before re-enabling ports.

Index