ENTERASYS NETWORKS™

NetSight

Element Manager

X-Pedition Router
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

Enterasys Networks 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.

trademark of Digital Equipment Corporation. **Novell** is a registered trademark of Novell, Inc. **CompuServe** is a registered trademark of CompuServe. **Sun Microsystems** is a registered trademark, and **Sun**, **SunNet**, and **OpenWindows** are trademarks of Sun Microsystems, Inc.

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, Inc., 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 4   Utilities

Index

Introduction

How to use this guide; related guides; getting help

Welcome to the Enterasys *NetSight Element Manager for the X-Pedition Router* (formerly the SmartSwitch Router). We have designed this guide to serve as a reference for using NetSight Element Manager for the X-Pedition 8000 (SSR-8), the X-Pedition 8600 (SSR-16), and the X-Pedition ER16.

The SSR-8 (8-slot chassis) and the SSR-16 (16-slot chassis) are Gigabit Ethernet switching routers that combine wire-speed performance, pinpoint control, and superior routing capabilities. The ER16 is a 16-slot chassis-based routing platform providing LAN/WAN backbone solutions.

NOTE
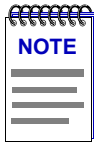
Since the devices covered by this user's guide are functionally similar, they will all be referred to as the X-Pedition Router.

Using the X-Pedition Router User's Guide

This guide contains information about management functions which are accessed directly from the X-Pedition Router's Device View.

Chapter 1, **Introduction**, provides a list of related documentation and shows you how to contact the Enterasys Global Technical Assistance Center.

Chapter 2, **The X-Pedition Router Device View**, describes the visual display of the router and the operation of chassis-level management functions, such as changing the chassis display and displaying statistics.

Chapter 3, **Statistics**, describes two port-level statistics options: RMON Ethernet Statistics and Interface Statistics.

Chapter 4, **Utilities**, describes two file transfer utilities for the X-Pedition Router: TFTP Download and Configuration Upload/Download.

While we provide as much background information as we can, we do assume that you're familiar with Ethernet IEEE 802.3 data communications networks and their physical layer components, and that you are familiar with general routing and switching concepts.

Related Manuals

If you have installed Netsight Element Manager on a Windows Platform system, you can access 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 include:

NetSight Element Manager User's Guide

NetSight Element Manager Tools Guide

NetSight Element Manager Remote Administration Tools User's Guide

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

NetSight Element Manager Alarm and Event Handling User's Guide

Network Troubleshooting Guide

For more information about the capabilities of the X-Pedition Router, consult the appropriate hardware documentation.

Getting Help

This section describes 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 **Help** buttons to obtain information specific to a particular window. 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 Device View menu bar, you can access on-line Help specific to the Device View. Refer to Chapter 2, **The X-Pedition Router Device View**, for information on the Device View.

Accessing On-line Documentation

If you have installed NetSight Element Manager on a Windows platform system, the complete suite of documents available for NetSight Element Manager can be accessed via a menu option available from the primary window menu bar: **Help—>Online Documents**. If you chose to install the documentation when you installed NetSight Element Manager, selecting this option will launch Adobe's Acrobat Reader and a menu file which provides links to all other available documents.

> **TIP**
>
> *If you have not yet installed the documentation, the* **Online Documents** *option will not be able to access the menu file; in order to activate this option, you must run the* setup.exe *again to install the documentation component. See your* **Installation Guide** *for details.*

Getting Help from the Global Technical Assistance Center

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

By phone: (603) 332-9400
24 hours a day, 365 days a year

By fax: (603) 337-3075
24 hours a day, 365 days a year

By mail: Enterasys Networks, Inc.
Technical Support
35 Industrial Way
Rochester, NH 03867

By e- mail: support@enterasys.com

FTP: ftp.ctron.com (134.141.197.25)

Login   `anonymous`
Password   `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 e-mail address:

Netsight_docs@enterasys.com

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

http://www.enterasys.com
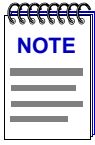
NOTE

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

The X-Pedition Router Device View

Information displayed in the Device View window; the Diagnostic Information window; statistics and chassis management functions

The Device View displays the current configuration of your X-Pedition Router chassis via a graphical display of the chassis front panel. The Device View displays each board installed in the chassis, and the condition of each individual port. The Device View also serves as a point of access to other X-Pedition Router windows.

To access the X-Pedition Router Device View, use one of the following options depending on whether you have NetSight Element Manager installed on a Windows® or Solaris® platform system.

Windows Platform:

If you have installed NetSight Element Manager on a Windows platform system, the device icon for the X-Pedition Router is displayed as shown in Figure 2-1.

Figure 2-1. The X-Pedition Router Icon

Access a Device View from the Element Manager main window:

1. In any map, list, or tree view, double-click on the X-Pedition Router you wish to manage.

    or

1. In any map, list, or tree view, click to select the X-Pedition Router you wish to manage.

2. Select **Manage—>Node** from the primary window menu bar, or select the Manage Node [icon] toolbar button.

   or

1. In any map, list, or tree view, click the **right** mouse button to select the X-Pedition Router you wish to manage.

2. On the resulting menu, click to select **Manage**.

You can also access a Device View outside of NetSight Element Manager:

1. From the Start Menu, select Start**—>**Programs**—>**Enterasys Networks**—>** NetSight Element Manager**—>**JavaDeviceManager. The Launch Device Manager window opens.

2. Enter the desired IP address and community name and click **OK**.

Solaris Platform:

If you have installed NetSight Element Manager on a Solaris Platform system, you can access a Device View from HP OpenView® Network Node Manager:

1. Right-click on the device icon you wish to manage and select Netsight Device Manager from the menu.

You can also access a Device View from the command line:

1. In your NetSight Element Manager installation directory, run DeviceManagerStandalone. You can also run DeviceManagerStandalone from your [home directory]/Enterasys Networks/Element Manager directory.

2. The Launch Device Manager window opens. Enter the desired IP address and community name and click **OK**.

Viewing Device Information

The Device View (Figure 2-2) provides a graphic representation of the X-Pedition Router, including a color-coded port display which informs you of the current status of all the ports on the boards installed in the device. Each port box can display a variety of information about the port (see **Selecting a Port View Display**, page 2-8).
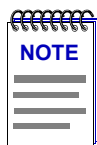
| NOTE | *If the total number of ports exceeds the number of ports that can be displayed at one time in the Device View, scroll arrows will appear, allowing you to scroll to view all of the ports.* |

Click on the board number to view the board menu.

Click on the port number to view the port menu.
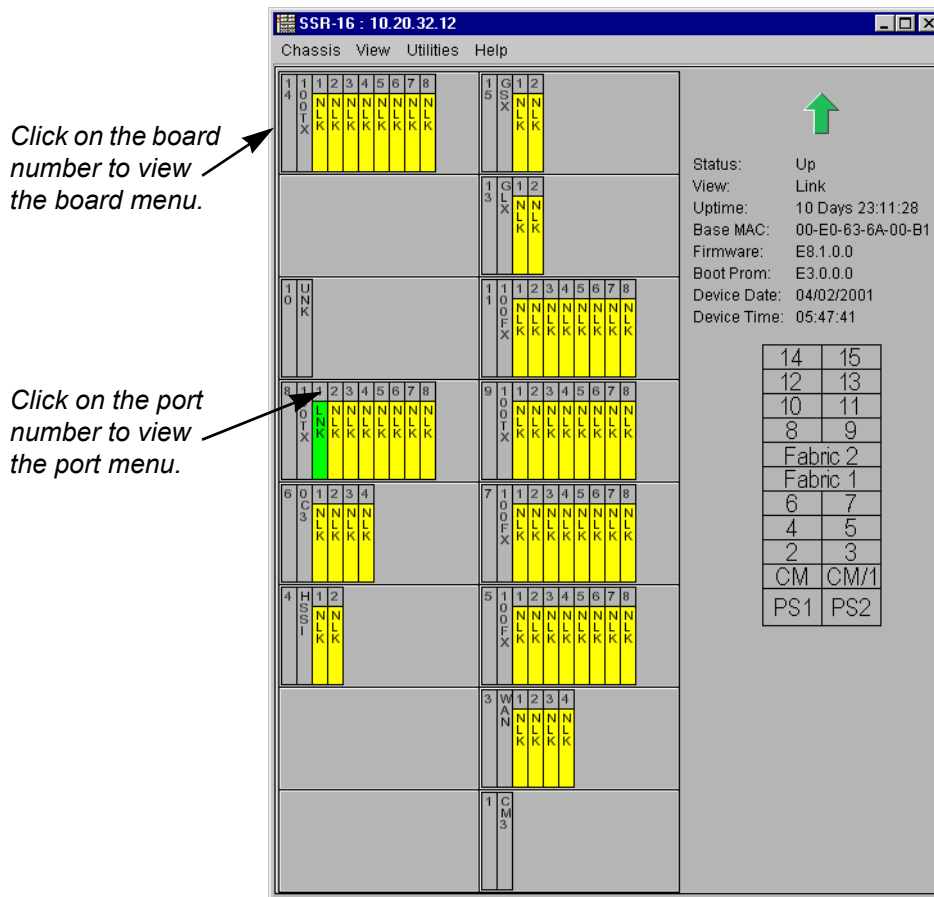
Figure 2-2. The X-Pedition Router Device View

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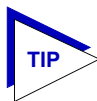
When you move the mouse cursor over a management "hot spot," the cursor icon will change into a hand symbol to indicate that clicking in the current location will bring up a management option.

Front Panel Information

In addition to the main interface display, the Device View window provides the following device information:

IP

The Device View window title displays the device's IP (Internet Protocol) Address. The IP address cannot be changed via NetSight Element Manager.

Connection Status

This color-coded arrow indicates the current state of communication between NetSight Element Manager and the X-Pedition Router. Clicking the icon refreshes the Device View and updates the display.

• **Up Arrow/Green** indicates the X-Pedition Router is responding to device polls (valid connection).

• **Hourglass/Beige** indicates Device Manager has lost contact with the device and is attempting to reconnect.

• **?/Yellow** indicates connection status in Unknown.

• **Down Arrow/Red** indicates the X-Pedition Router is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

Status

Displays the current status of the chassis: Up, Down, Standby, or Unknown

View

Indicates the port display option currently in effect. The default port status view is Link; if you have not changed the port status selection since launching the Device View window, this field will display. For more information about changing the port status display, see **Selecting a Port View Display**, page 2-8.

UpTime

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

Base MAC

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

Firmware

The revision of device firmware stored in the X-Pedition Router's FLASH PROMs.

Boot Prom

The revision of Boot Prom installed in the X-Pedition Router.

Device Date

The current date in mm/dd/yyyy format, in the internal clock of the device.

Device Time

The current time in hh:mm:ss format, in the internal clock of the device.

Chassis Display

A graphical depiction of the chassis layout indicating the placement of boards, control modules, and power supplies. (This is not included in the Device View for the ER16.)

Menu Structure

By clicking on various areas of the X-Pedition Router Device View, you can access menus with chassis-, board-, and port-level options, as well as utility applications which apply to the device. The following illustration displays the menu structure and indicates where to click the mouse to access the various menus:
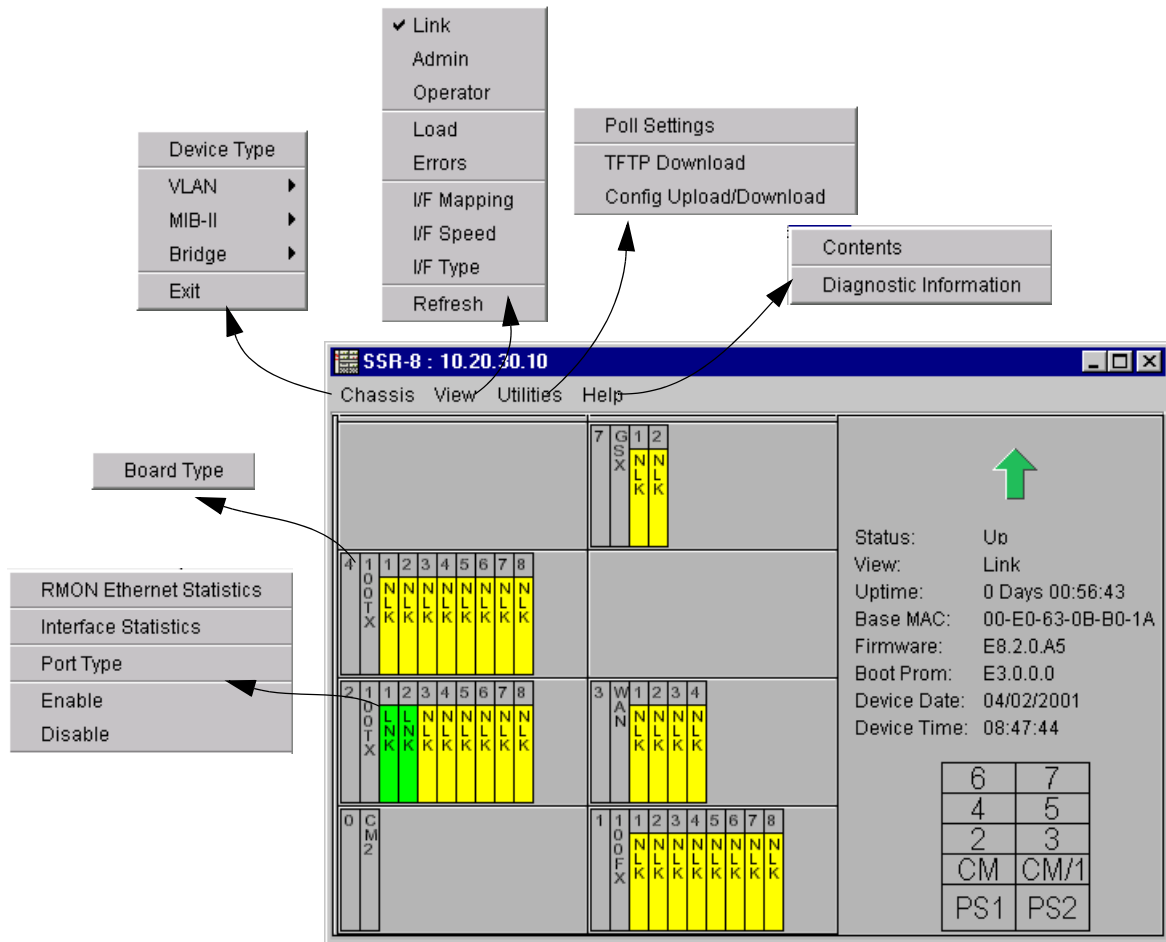

Figure 2-3. X-Pedition Router Device View Menu Structure

The Chassis Menu

Clicking on **Chassis** on the Device View window menu bar displays the Chassis menu, where you can access the following selections:

- **Device Type** displays a window containing a physical hardware description of the device (see **Viewing Hardware Types**, page 2-11).

- **VLAN—>VLAN Configuration** opens the VLAN Configuration window where you can add and delete VLANs, configure VLAN IDs and names, and enable or disable VLANs.

- **VLAN—>VLAN Port Configuration** opens the VLAN Port configuration (Basic) window where you can configure basic VLAN port parameters such as VLAN name, egress state, and Acceptable Frame Types. You can also access advanced VLAN port parameters from this window.

- **VLAN—>VLAN Port Egress Configuration** opens the VLAN Egress Port Configuration window which lets you select a VLAN on the device, and display the ports whose egress lists contain the selected VLAN. The window also allows you to change the egress state for each port.

- **MIB-II—>Interface Summary** opens the Interface Summary window which provides an overview of interface information for each port on the device. You can also access detailed Interface Statistics from this window.

- **MIB-II—>SNMP Group** opens the SNMP Group window where you can view statistical information concerning SNMP (Simple Network Management Protocol) defined objects on your device.

- **MIB-II—>System Group** opens the System Group window where you can enter the device name, location, and contact person. You can also view the SysORTable which defines the Agents-Capabilities (A-C) statement for the device.

- **Bridge—>Bridge Summary** opens the Bridge Summary window where you can view the current status of bridging across your device and view information on each bridge port.

- **Bridge—>Bridge Filtering Database** opens the Bridge Filtering Database window where you can add or delete entries from the Filtering Database and configure filtering information for each entry.

- **Bridge—>Bridge Spanning Tree** opens the Bridge Spanning Tree Configuration window where you can view and modify bridge port- and device-level information relating to the Spanning Tree Algorithm.

- **Bridge—>Find Source Address** opens the Find Source Address window used to locate the source port for a specific MAC address on the selected device. See **Using the Find Source Address Option**, page 2-14, for details.

- **E<u>x</u>it** closes the Device View.

The View Menu

The View menu allows you to select the status information that will be displayed in the port boxes in the Device View:

- **Link** displays the port's link state.

- **Admin** displays the port's admin state.

- **Operator** displays the port's operator state.

- **Load** display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits/sec, or 1.00 Gbits/sec) of the connected network.

- **Errors** displays the number of errors detected per polling interval by each port as a percentage of the total of number of valid packets processed by the port.

- **I/F Mapping** displays the interface index associated with each port.

- **I/F Speed** displays the bandwidth of each individual port: 10M (megabits) for standard Ethernet, 100M for Fast Ethernet, and 1.00G for Gigabit Ethernet.

- **I/F Type** displays the interface type of each port.

- **Refresh** updates the information displayed in the Device View.

For more information on the port display options available via this menu, see **Port View Displays**, page 2-8.

The Utilities Menu
The Utilities menu provides access to utilities to assist in managing the X-Pedition Router.

- **Poll Settings** opens the Poll Setting window where you can display and configure polling settings for the Device Manager.

- **Config Upload/Download** opens the Configuration Upload/Download window where you can upload or download a configuration file.

- **TFTP Download** opens the TFTP Download window where you can download a new firmware image.

The Help Menu
The Help Menu provides the following option:

- **Contents** displays the NetSight Element Manager Help Contents.

- **Diagnostic Information** provides information that is useful when troubleshooting NetSight Element Manager functionality.

The Board Menu
The Board menu provides the following option:

- **Board Type** displays a physical hardware description of the board.

The Port Menu
Each port menu offers the following selections:

- **RMON Ethernet Statistics** displays the RMON Ethernet Statistics window where you can view a detailed statistical breakdown of traffic on the monitored Ethernet network segment. RMON must be enabled through the router's local management.

- **Interface Statistics** displays the Interface Statistics window where you can view color-coded statistical information about the port.

• **Port Type** displays a description of the selected port (see **Viewing Hardware Types**, page 2-11).

• **Enable/Disable** administratively turns the selected port on or off.

Port View Displays

Each port display on the X-Pedition Router will indicate that port's current state. When you open the Device View, each port will display its Link status (defined below). To change the port View display, select one of the options on the View menu, as described in the following sections.

Selecting a Port View Display

To change the view display of your ports:

1. Click on **View** in the Device View menu bar.

2. Select the port view information you want to display. The port text boxes will display the appropriate status information.

Port view options are:

Link
Displays the port's link state:

LNK (green)	Link
NLK (yellow)	No Link (the default port display when you open the Device View)
TST (yellow)	Testing mode
UNK (yellow)	Unknown, the device returns the value Unknown
UNK (light gray)	Unknown, the device is returning a value that the software does not recognize
DRMT (yellow)	Dormant; the interface is waiting for external actions (such as a serial line waiting for an incoming connection
NPST (yellow)	Not Present; the interface has missing components (usually hardware)
DWN (red)	Lower Layer Down; the interface is down due to the state of lower-layer interface(s)
blank (dark gray)	the device is not responding

Admin

Displays the port's Admin state:

ON (green)	the port has been administratively enabled
OFF (red)	the port has been administratively disabled
TST (yellow)	the port has been administratively placed in a test mode
UNK (light gray)	unknown; device is returning a value that the software does not recognize
blank (dark gray)	the device is not responding.

Operator

Displays the port's Operator state:

ON (green)	Operational status up
OFF (red)	Operational status down
TST (yellow)	Operational status testing; no operational packets can be passed
UNK (yellow)	Unknown, the device returns the value Unknown
UNK (light gray)	Unknown, the device is returning a value that the software does not recognize
DRMT (yellow)	Dormant; the interface is waiting for external actions (such as a serial line waiting for an incoming connection
NPST (yellow)	Not Present; the interface has missing components (usually hardware)
DWN (red)	Lower Layer Down; the interface is down due to the state of lower-layer interface(s)
blank (dark gray)	the device is not responding

Load

Display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits/sec, or 1.00 Gbits/sec) of the connected network.

Errors

Display the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors generated during the last polling interval by devices connected to that port compared to the total number of valid packets processed by the port.

I/F Mapping

Display the interface index (the MIB II *ifIndex* value) associated with each port on the X-Pedition Router chassis.

I/F Speed

Display the bandwidth of each individual port in the X-Pedition Router: 10M (megabits) for standard Ethernet; 100M for Fast Ethernet; and 1.00G for Gigabit Ethernet.

I/F Type

Display the interface type of each port in the X-Pedition Router chassis, for example, Ethernet (Eth). Note that there is no type distinction between Ethernet, Fast Ethernet, or Gigabit Ethernet.

Port Status Color Codes

The ports display different information depending on what View Menu port display option is selected. The display is color-coded for three of the options: Link, Admin, and Operator. All other options will continue to reflect the most recently selected option that does use color-coding.

The Diagnostic Information Window

The Diagnostic Information window provides information that is useful when troubleshooting NetSight Element Manager functionality. Like most networking devices, Cabletron and Enterasys devices draw their functionality from a collection of MIBs. The MIB tab of the Diagnostic Information window, Figure 2-4, displays the MIBs — and, therefore, the functionality — supported by the currently monitored device.

To view the Diagnostic Information window:

1. Click on **Help** in the Device View menu bar.

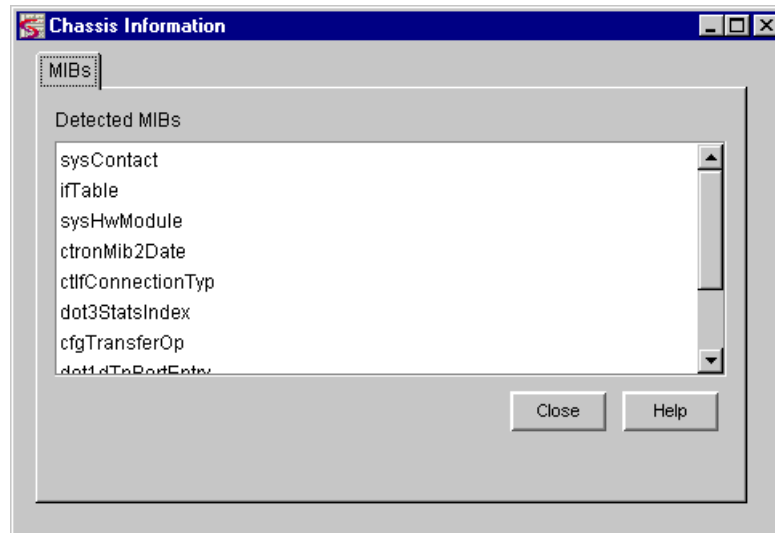2. Select **Diagnostic Information** from the menu.

Figure 2-4. Diagnostic Information Window

Viewing Hardware Types

In addition to the graphical displays described above, certain menu options provide specific information about the physical characteristics of ports and boards in the X-Pedition Router, as well as information about the device itself.

Device Type

Choosing the **Device Type** option on the Chassis menu brings up a window that describes the management device being modeled:
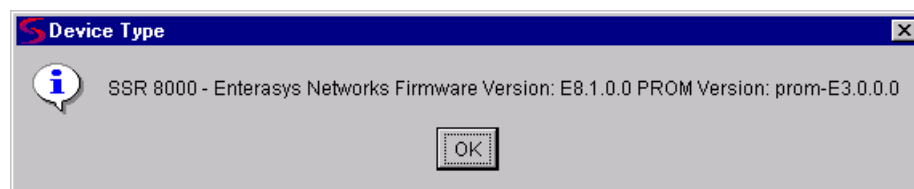

Figure 2-5. Device Type Window

Board Type

From the Board menu in the Device View window, you can view a description of the board type in your device.

To view a board type:

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

2. Click on **Board Type**. A Board Type window, similar to the example shown in Figure 2-6, will appear.
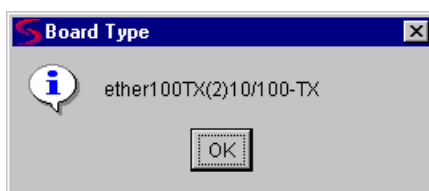
Figure 2-6. Board Type Window

Port Type

You can view a brief description of the ports on your X-Pedition Router via the Port Type selection on the Port menu.

To view a Port description:

1. Click on the appropriate port to display the Port menu.

2. Click on **Port Type**. A Port Type window, similar to the sample shown in Figure 2-7, will appear with a description of the port interface. The port is identified first by a text description of the type of interface (physical port), the type of the interface: ethernet (et); v.35 (se); High Speed Serial Interface (hs); or Gigabit Ethernet (gi), followed by the board number and port number.
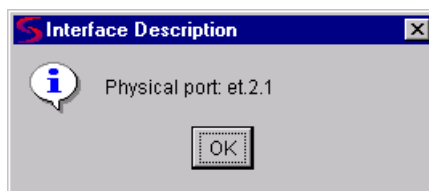
Figure 2-7. Port Type Window

Viewing Interface Summary Information

The **Interface Summary** menu option available from the Chassis menu lets you view information about each port interface on your device. The window also provides access to a detailed Interface Statistics window that breaks down Transmit and Receive traffic for each interface. (See Chapter 3, **Interface Statistics** for more information.)

To access the Interface Summary window:

1. From the Device View, click on the **Chassis** option from the menu bar and select **MIB-II—>Interface Summary** from the menu.

2. The Interface Summary window, Figure 2-8, opens.

Figure 2-8. Interface Summary Window

The Interface Summary window provides a variety of descriptive information about each interface on your device:

Interface
Displays the index value assigned to each port interface on the device.

Type
Displays the type of port interface.

Description
Displays a description of the port, the type of interface followed by the board number and port number.

Physical Status
Displays the current physical status — or operational state — of the interface:

On   the operational status is up

Off	the operational status is down
Dormant	the interface is waiting for external actions (such as a serial line waiting for an incoming connection)
Lower Layer Down	the interface is down due to the state of lower-layer interface(s)
Not Present	the interface has missing components (usually hardware)
Testing	operational status testing; no operational packets can be passed
Unknown	the device is returning the value Unknown or a value that the software does not recognize

Logical Status

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

Address

Displays the physical (MAC) address of the port interface.

Speed

Displays an estimate of the interface bandwidth in bits per second. For an interface that either does not vary in bandwidth or where an accurate estimation cannot be made, this field displays the lowest bandwidth available.

Using the Find Source Address Option

When you select the **Find Source Address** option, the device's 802.1d Filtering Database is searched for the specified MAC address. If it is found, the **Component** field will display the value "Bridge" indicating that the address was found on a bridging interface, and the **Port Instance** field will display the index number assigned to the bridge port on which the address was located.

NOTE
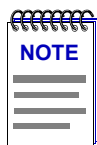
You may receive an error message stating "Can't Display Source Address" if a Port Instance of "0" or "0.0" is reported. This value indicates that the MAC address is communicating through the backplane instead of through a front panel interface.

To open the Find Source Address window:

1. Click on **Chassis** in the Device View menu bar.

2. Click on **Bridge—> Find Source Address**. The Find Source Address window, as shown in Figure 2-9, opens.
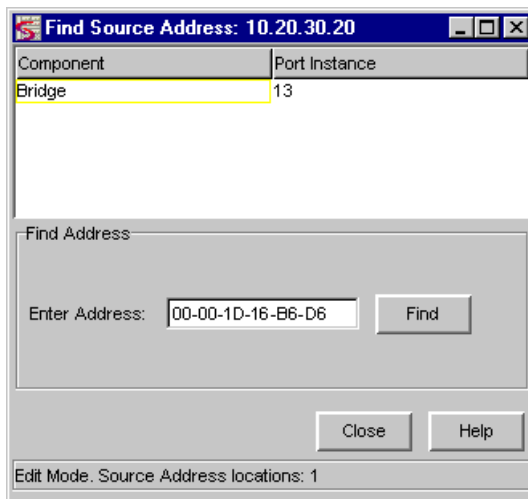
Figure 2-9. Find Source Address Window

The Find Source Address window displays the following information:

Component
Displays the type of interface through which the specified MAC address is communicating. This field will report **Bridge**.

Port Instance
Displays the bridge port index number on which the specified MAC address was found. Bridge port index numbers may not match interface port index numbers (the MIB-II *ifIndex* value) because there is an offset in the mapping between the two. Use a MIB tool to query *dot1dBasePortIfIndex* (1.3.6.1.2.1.17.1.4.1.2) and view the mapping and offset.

To use the Find Source Address window:

1. In the **Enter Address** field, enter the Source Address you wish to find in the appropriate XX-XX-XX-XX-XX-XX format.

2. Click **Find**.

If the specified MAC address is located, a list of the interface(s) through which the given address is communicating appears in the list box. A status message at the bottom of the window displays the number of interfaces through which the given MAC address is communicating.

If the specified MAC address cannot be found, a "**Source Address not found**" message will appear.

Managing the Chassis

In addition to the performance and configuration information described in the preceding sections, the Device View also provides you with the tools you need to configure your X-Pedition Router and keep it operating properly. Management functions include configuring 802.1Q VLANs, enabling and disabling ports, and poll settings.

802.1Q VLANs

This section introduces and describes IEEE 802.1Q VLAN (Virtual Local Area Network) technology on the X-Pedition Router.

What is a VLAN?

A VLAN is a logical group of devices that function as a single Local Area Network segment (broadcast domain). Devices comprising a VLAN may be (physically) widely separated, allowing users located in separate areas or connected to separate ports to belong to a single VLAN group. Users assigned to a VLAN can send and receive broadcast and multicast traffic as though they were all physically connected to a single network segment. VLAN-capable switches isolate broadcast and multicast traffic received from VLAN groups, and contain broadcasts and multicasts from members of a VLAN within that group.

Switches that support IEEE 802.1Q VLANs act by classifying frames into VLAN membership. Usually, VLAN classification is based on tag headers (VLAN tags) in the headers of data frames. The tag header is inserted into the frame directly after the Source MAC address field. A four-byte field in the tag header is used as the VLAN identifier. These VLAN tags are added to data frames by the switch as the frames are transmitted and/or received by certain ports, and are later used to make forwarding decisions by the switch and other 802.1Q switches. In the absence of a VLAN tag, a frame is assigned VLAN membership according to the VLAN configuration of the switch port that receives the frame.

About 802.1Q VLAN Configuration and Operation

An 802.1Q VLAN is defined by assigning it a unique identification number (the VLAN ID) and a VLAN name. The VLAN ID is used to identify data frames that originate from, and are intended for, the ports assigned to the VLAN. Up to 1024 VLANs may be created, with VLAN IDs ranging from 2-4094. VLAN ID 1 is reserved for the Default VLAN.

Ports on 802.1Q switches are assigned membership in a VLAN by associating a VLAN ID with each port on the switch. When you assign a VLAN to a port, that VLAN's ID becomes the Port VLAN ID (PVID) for the port. Initially, all ports are associated with the Default VLAN (VLAN ID 1).

Once VLANs have been configured and activated, all frames with unknown destination addresses (including broadcast, unknown multicast, and unknown unicast frames) will be contained within the VLAN of their origin. The switch's Filtering Database tracks the associations between MAC addresses, VLAN eligibilities, and port numbers, and is used to make forwarding decisions for frames. All VLANs share a single Spanning Tree.

Ingress List Operation

A port's ingress list specifies the VLAN with which received frames will be associated. The switch's Filtering Database tracks the associations between VLAN eligibilities, MAC addresses, and port numbers.

Untagged frames received by an 802.1Q switch port are classified according to the VLAN membership of the port that receives the frame.

Tagged frames received by an 802.1Q switch port are forwarded according to the VLAN indicated in their tag header. A port may receive a tagged frame that specifies a VLAN other than the one assigned to the port.

Egress List Operation

Each port's egress list specifies which VLANs are associated with the port, and specifies what type of frame (tagged and/or untagged) to transmit for each particular VLAN on a port.

VLAN Configuration

Define your VLANs using the VLAN Configuration window, which allows you to add and delete VLANs, configure VLAN IDs and names, and enable or disable VLANs.

After your VLANs are defined, you can configure basic and advanced VLAN parameters and VLAN port egress lists using the VLAN Port Configuration windows and the VLAN Egress Port Configuration window, respectively.

Setting VLAN Parameters and Status

The VLAN Configuration window allows you to view, create, modify, delete, enable, and disable VLANs on the device. To launch the window:

1. Click on **Chassis** in the Device View menu bar.

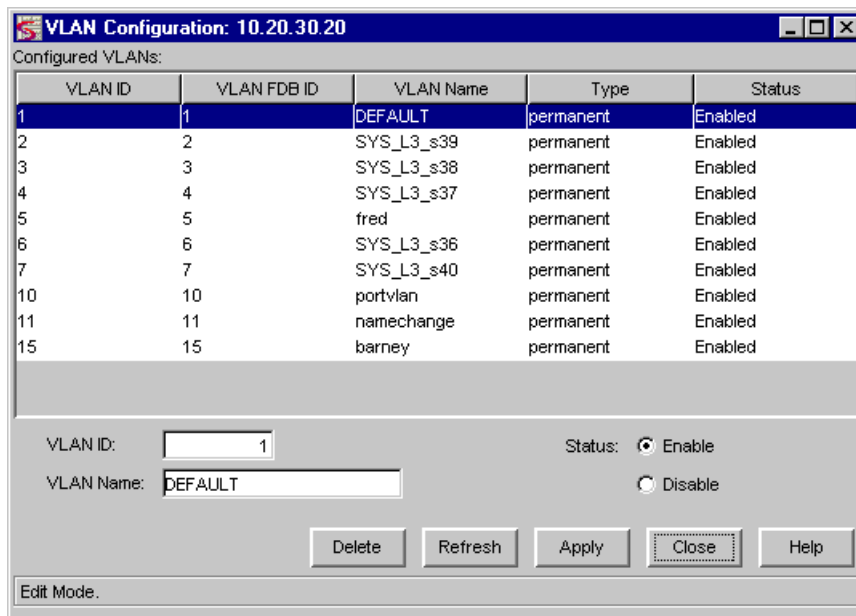2. Click on **Bridge—> VLAN Configuration**. The VLAN Configuration window, Figure 2-10, appears.

Figure 2-10. The VLAN Configuration Window

The **Configured VLANs** table displays the following information about VLANs configured on the module:

VLAN ID
Displays the unique number that identifies the VLAN. Allowable values range from 2 to 4094. VLAN ID 1 is reserved for the default VLAN.

VLAN FDB ID
Displays the unique number that identifies the VLAN's Filtering Database (FDB).

VLAN Name
Displays the name (up to 32 characters) assigned to the VLAN.

Type
Displays the VLAN type: Permanent (the VLAN is active and will remain so after the next reset of the device), Dynamic GVRP (the VLAN is active and will remain so until removed by GVRP), or other (the VLAN is active, but is not permanent or dynamic GVRP).

Status
Displays the current status of the selected VLAN: Enabled (active), Disabled (not active), or Other (created but turned off or in the process of being created).

Creating and Modifying VLANs

The fields immediately below the **Configured VLANS** table are used to create and modify your VLANs. To create a new VLAN:

1. In the **VLAN ID** field, enter a unique value between **2**-**4094**. VLAN ID **1** is reserved for the Default VLAN, and cannot be used.

2. Enter a name for the VLAN in the **VLAN Name** field. VLAN names must be 32 characters or less.

3. Click the **Apply** button. The new VLAN will be added to the **Configured VLANs** table.

Once a VLAN has been created, its VLAN ID cannot be modified. If you wish to change a VLAN's ID, you'll have to delete the VLAN and create a new entry. See **Deleting VLANs**, below, for instructions on deleting a VLAN.

To modify an existing VLAN's name, select its entry in the **Configured VLANs** table. The selected VLAN's name will be displayed in the **VLAN Name** field. Modify the displayed name as outlined in Steps 2-3, above.

Deleting VLANs

The VLAN Configuration window also allows you to delete VLANs (except for the Default VLAN, which cannot be deleted). When a VLAN is deleted, any ports assigned to that VLAN will automatically become members of the Default VLAN. To delete a VLAN:

1. Select the desired VLAN entry in the **Configured VLANs** table.

2. Click the **Delete** button. The selected VLAN will be removed.

Enabling and Disabling VLANs

To enable or disable VLANs:

1. Select the desired VLAN entry in the **Configured VLANs** table.

2. In the **Status** field, select **Enable** or **Disable**.

3. Click the **Apply** button. The selected VLAN will be enabled or disabled, depending on your selection.

Updating VLAN Configuration Window Information

Clicking the **Refresh** button will update the information displayed in the Configured VLANs table without closing the window.

Configuring Basic VLAN Port Parameters

VLAN port assignment and Acceptable Frame Types configuration is performed using the VLAN Port Configuration (Basic) window. You can also use this window to access Advanced VLAN Port parameters using the **Advanced** button at the bottom of the window. To launch the window:

1. Click on **Chassis** in the Device View menu bar.

2. Click on **Bridge—> VLAN Port Configuration**. The VLAN Port Configuration (Basic) window, Figure 2-11, opens:
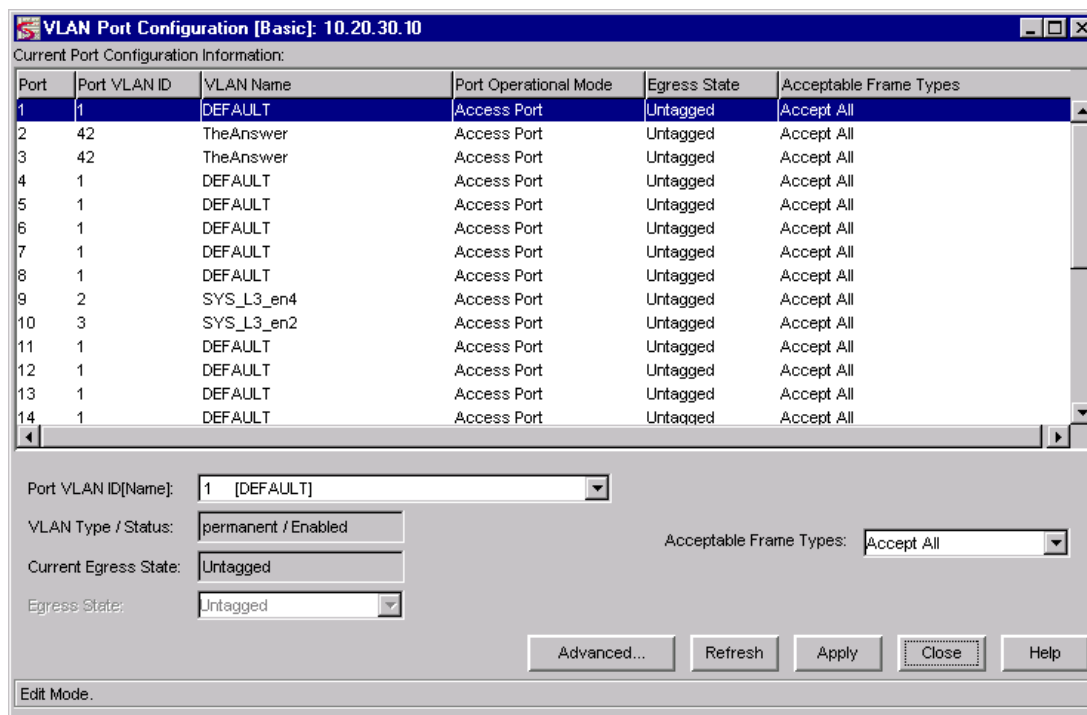

Figure 2-11. The VLAN Port Configuration (Basic) Window

The window displays the following information:

Port
Displays the number that identifies the port.

Port VLAN ID
Displays the VLAN ID and name of the VLAN assigned to the port. When you assign a VLAN to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port. Endpoints connected to the port become members of that VLAN. All untagged frames received on the port are tagged with the PVID, unless a classification rule exists for the frame's classification type.

VLAN Name

Displays the name (up to 32 characters) assigned to the selected VLAN.
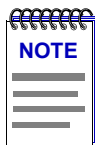
Operational Mode

Displays the port's operational mode:

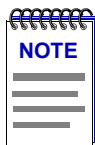|	
Access Port	the port's Acceptable Frame Types is Accept All, its Egress State is Untagged, and its PVID is the Default VLAN
Trunk Port	the port's Acceptable Frame Types is Accept Tagged, its Egress State is Tagged, and its PVID can be any VLAN

Egress State

Displays the current egress state for the port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

> **NOTE**
>
> *On the X-Pedition Router, the Egress State is configured automatically by the device according to the Acceptable Frame Types state, and can also be configured by the user in the VLAN Egress Port Configuration window.*

Acceptable Frame Types

Displays a port's Acceptable Frame Type setting: Accept All (the port accepts both tagged and untagged frames), or Accept Tagged (the port accepts only tagged frames).

> **NOTE**
>
> *On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.*

Assigning VLAN Membership to Ports
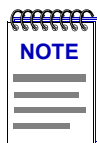
To assign a port to any configured VLAN:

1. In the table, select a port that you wish to assign to a VLAN. The port's current VLAN configuration information, including its VLAN ID, will be displayed in the fields below.

2. In the **Port VLAN ID** field, use the drop-down list to select the VLAN ID of the VLAN to which you wish to assign the selected port.

3. Click the **Apply** button. The new VLAN assignment will be reflected in the VLAN Port Configuration (Basic) window's table.

Setting a Port's Acceptable Frame Types

To set a port's Acceptable Frame Types:

1. Select the desired port in the table:

2. Use the Acceptable Frame Types drop-down list to select: Accept All (the port accepts both tagged and untagged frames), or Accept Tagged (the port accepts only tagged frames). If the port does not support this functionality, the field will be grayed out.

3. Click the **Apply** button. The new state will be reflected in the VLAN Port Configuration (Basic) window's table.

> **NOTE**
>
> *On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.*

Updating VLAN Port Configuration Information

Clicking the **Refresh** button will update the information displayed in the Port Configuration table without closing the window.

Configuring Advanced VLAN Port Parameters

Additional VLAN port configuration is performed using the VLAN Port Configuration (Advanced) window, which is accessed from the VLAN Port Configuration (Basic) window. To launch the window:

1. Click on **Chassis** in the Device View menu bar.

2. Click on **Bridge—> VLAN Port Configuration**. The VLAN Port Configuration window opens.

3. At the bottom of the VLAN Port Configuration window, click the **Advanced** button. The VLAN Port Configuration (Advanced) window, Figure 2-12, appears:
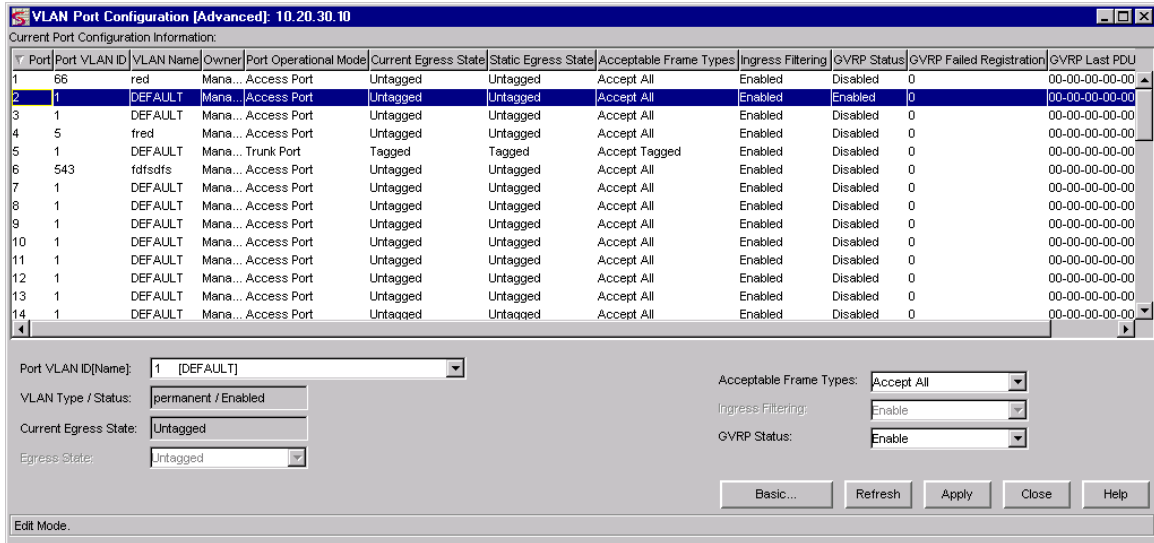
Figure 2-12. The VLAN Port Configuration (Advanced) Window

The window displays the following information:

Port
Displays the number that identifies the port.

Port VLAN ID
Displays the VLAN ID of the VLAN assigned to the port. When you assign a VLAN to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port. Endpoints connected to the port become members of that VLAN. All untagged frames received on the port are tagged with the PVID, unless a classification rule exists for the frame's classification type.

VLAN Name
Displays the name (up to 32 characters) assigned to the selected VLAN.

Owner
Specifies how the port's egress state was configured: by management, by GVRP (GARP VLAN Registration Protocol), or by Dynamic Egress.

Operational Mode
Displays the port's operational mode:

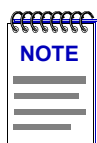|	
Access Port	the port's Acceptable Frame Types is Accept All, its Egress State is Untagged, and its PVID is the Default VLAN
Trunk Port	the port's Acceptable Frame Types is Accept Tagged, its Egress State is Tagged, and its PVID can be any VLAN

Current Egress State

Displays the current egress state for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).
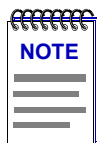
Static Egress State

Displays the static egress state for the port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

> **NOTE**
>
> *On the X-Pedition Router, the Egress State is configured automatically by the device according to the Acceptable Frame Types state, and can also be configured by the user in the VLAN Egress Port Configuration window.*

Acceptable Frame Types

Displays a port's Acceptable Frame Types setting: Accept All (the port accepts both tagged and untagged frames), Accept Tagged (the port accepts only tagged frames) or No Capability (the port does not support this functionality).

> **NOTE**
>
> *On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.*

Ingress Filtering

On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

GVRP Status

Displays whether GVRP (GARP VLAN Registration Protocol) is currently enabled or disabled on the port. GVRP is a protocol used to dynamically add VLANs to port egress lists across a domain. Ports that do not support this functionality will display N/A.

GVRP Failed Registration

Displays the total number of failed GVRP registrations for all VLANs on the port. Ports that do not support this functionality will display N/A.

GVRP Last PDU Origin

Displays the source MAC Address of the last GVRP message (PDU, Protocol Data Unit) received on the port. Ports that do not support this functionality will display N/A.
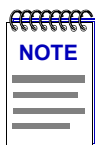
Assigning VLAN Membership to a Port

To assign a port to any configured VLAN:

1. In the table, select a port that you wish to assign to a VLAN. The port's current VLAN configuration information, including its VLAN ID, is displayed in the fields below.

2. In the **VLAN ID** field, select the VLAN ID of the VLAN to which you wish to assign the selected port.

3. Click the **Apply** button. The new VLAN assignment will be reflected in the VLAN Port Configuration (Advanced) window's table.

Setting a Port's Acceptable Frame Types

To set a port's Acceptable Frame Types:

1. Select the desired port in the table:

2. Use the Acceptable Frame Types drop-down list to select: Accept All (the port accepts both tagged and untagged frames), or Accept Tagged (the port accepts only tagged frames). If the port does not support this functionality, the field will be grayed out.

3. Click the **Apply** button. The new state will be reflected in the VLAN Port Configuration (Advanced) window's table.

NOTE

On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.

Configuring GVRP

To enable or disable GVRP (GARP VLAN Registration Protocol) on a port:

1. Select the desired port in the table:

2. Use the GVRP drop-down list to specify whether GVRP will be enabled on the port. GVRP is a protocol used to dynamically add VLANs to port egress lists across a domain. If the device does not support GVRP, this field will be grayed out.

3. Click the **Apply** button. The new state will be reflected in the VLAN Port Configuration (Advanced) window's table.

Updating VLAN Port Configuration Information

Clicking the **Refresh** button will update the information displayed in the Port Configuration table without closing the window.

Performing Egress List Configuration

Ports can transmit traffic for any or all defined VLANs on your network as long as the VLANs are on the port's egress list. Use the VLAN Egress Port Configuration window to determine which VLANs are on each port's egress list. To launch the window:

1. Click on **Chassis** in the Device View menu bar.

2. Click on **Bridge—> VLAN Egress Port Configuration**. The VLAN Egress Port Configuration window, Figure 2-13, appears:
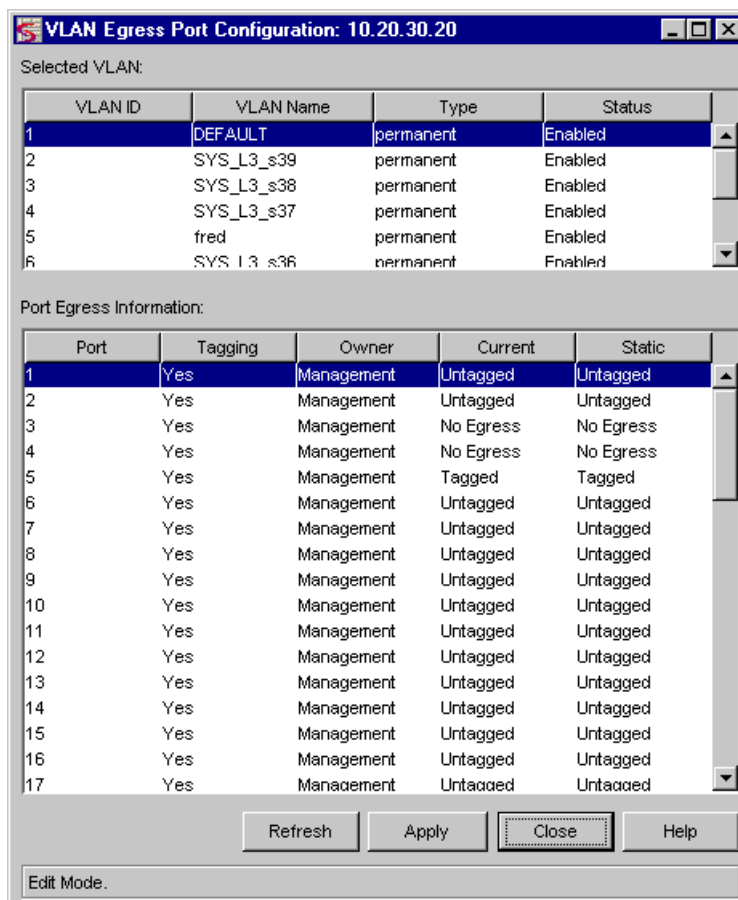

Figure 2-13. The VLAN Egress Port Configuration Window

The **Selected VLAN** table at the top of this window lists the VLANs currently configured on the device. You can select a VLAN from this list to associate with the egress lists on the device's ports. The Selected VLAN table includes the following information:

VLAN ID
The unique identifier for the VLAN.

VLAN Name
The name assigned to the VLAN.

Type
Displays the VLAN type: Permanent (the VLAN is active and will remain so after the next reset of the device), Dynamic GVRP (the VLAN is active and will remain so until removed by GVRP), or other (the VLAN is active, but is not permanent or dynamic GVRP).

Status
Displays the current status of the selected VLAN: Enabled (active), Disabled (not active), or Other (created but turned off or in the process of being created).

The **Port Egress Information** table lists the ports whose egress lists contain the selected VLAN. You can use this list to change how frames belonging to the selected VLAN will be forwarded out a port.

Port
Displays the number that identifies the port.

Tagging
Displays whether the port is implementing the 802.1Q VLAN functionality of tagging frames and GVRP (GARP VLAN Registration Protocol).

Owner
Specifies how the port's egress state was configured: by local management, by GVRP (GARP VLAN Registration Protocol), or by Dynamic Egress.

Current
Displays the current egress state for the port. The egress state specifies how frames belonging to the selected VLAN are forwarded out the port: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged).

Static
Displays the desired egress state for the port: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged). Right-mouse click on the port to select the desired egress state from the menu.

Configuring Egress State

To configure the egress state (how frames will be transmitted) for the ports on the board:

1. In the Selected VLAN table at the top of the VLAN Egress Port Configuration window, click to select a VLAN. The ports that contain this VLAN in their egress lists are displayed in the lower portion of the window.

2. In the Port Egress Information list, right-click the desired port, and select the egress state: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged). To change the egress state for all the ports listed, right-click a port and select All No Egress, All Tagged, or All Untagged.

3. Repeat for another VLAN, if desired.

4. Click **Apply** to set the change(s).
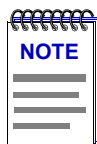
NOTE	*When setting egress state, remember that Access ports cannot be set to tagged, and Trunk ports cannot be set to untagged.*
	Egress state cannot be set by the user on X-Pedition Routers with firmware versions of E8.1.0.0 or earlier.

Enabling and Disabling Ports

When you disable bridging at a port interface, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge or with other networks connected to the bridge. When you enable bridging for the interface, the port moves from the Disabled state through the Listening and Learning states to the Forwarding state.

To enable or disable bridging for an individual interface:

1. Click on the appropriate port display box to display the Port menu.

2. Click to select **Enable** to enable bridging at the interface, or **Disable** to disable bridging. Bridging will now be enabled or disabled across the selected port, as desired.

Configuring Poll Settings

Use the Poll Setting window to display and configure how Device Manager polls monitored devices.

1. Click on **Utilities** in the Device View menu bar.

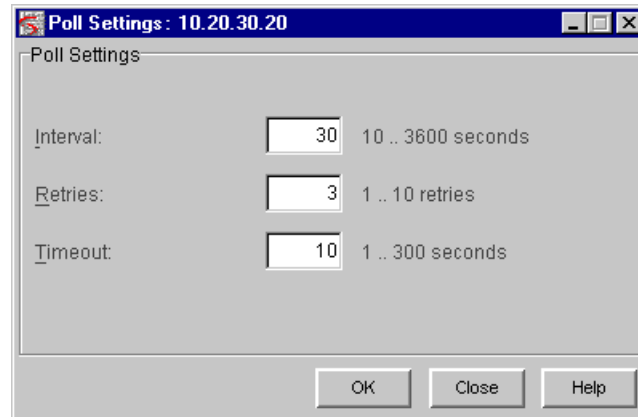2. Select **Poll Settings** from the menu. The Poll Settings window, Figure 2-13, opens:

Figure 2-14. The Poll Settings Window

The window allows you to configure the following poll settings:

Interval
Displays the time that Device Manager waits between attempts to contact the device.
Allowable values are 10 to 3600 seconds.

Retries
Displays the number of unsuccessful polls that take place before Device Manager issues
an alarm. Allowable values are 1 to 10 retries.

Timeout
Displays the amount of time that Device Manager waits between polling retries.
Allowable values are 1 to 300 seconds.

To configure the poll settings:

1.   In the Poll Settings window, enter the desired values in the fields.

2.   Click **OK** to configure the settings and close the window.

Statistics

RMON Ethernet Statistics and Interface Statistics

The Device View for the X-Pedition Router provides two port-level statistics options: **RMON Ethernet Statistics** and **Interface Statistics**.

RMON Ethernet Statistics

The RMON Ethernet Statistics window (Figure 3-1) provides a detailed statistical breakdown of traffic on a monitored Ethernet network.
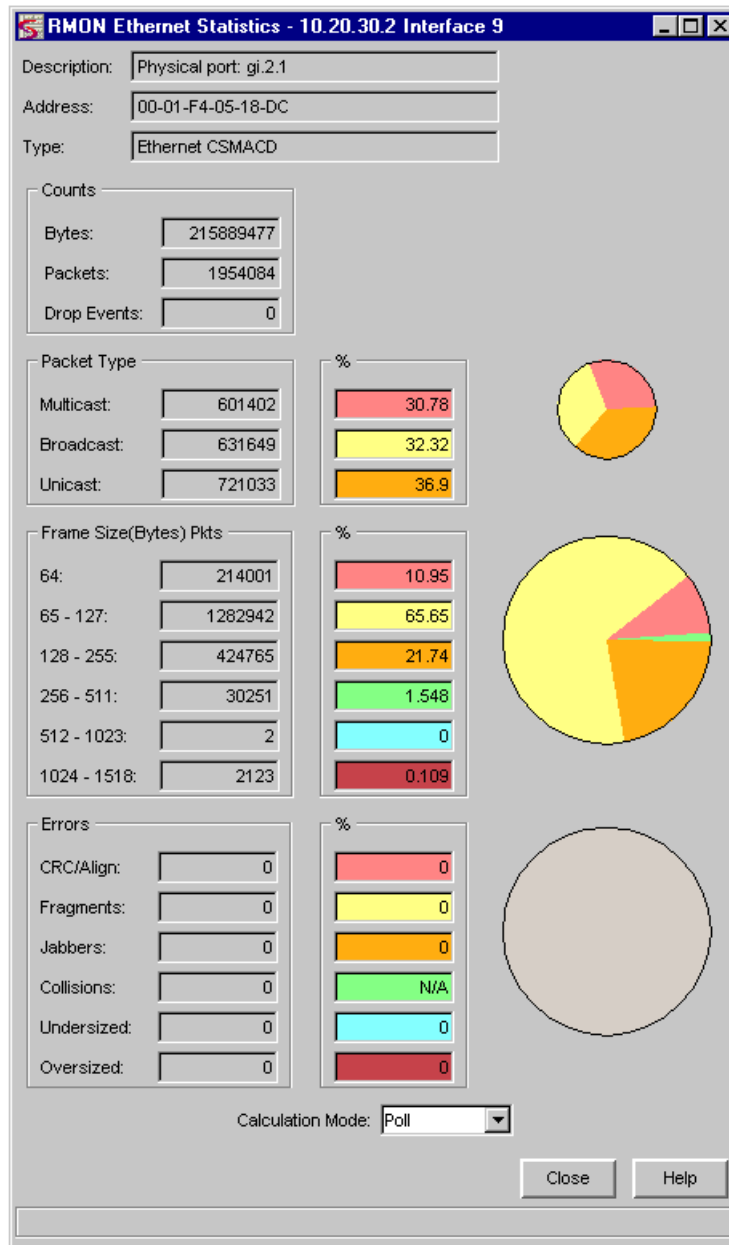
Figure 3-1. The RMON Ethernet Statistics Window

When viewing this window, keep in mind that the data provided applies only to the interface or network segment. If you reset your device, close and re-open this window to refresh the values.

The selected interface number and its description are displayed at the top of the window. Below, the statistics are displayed as total counts, and for some, as percentages. The pie charts present a graphical view of the percentage breakdown and the colors in the pie chart correspond to the colors in the percentage display boxes.

You can choose whether to view the total statistics count (since the last time the device was initialized), the statistics count during the last polling interval, or a fresh accumulation of statistics. See **Viewing Total, Delta, and Accumulated Statistics**, on page 3-5, for more information.

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

Description
Displays a description of the type of interface followed by the board and port number.

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

Type
The type of interface, distinguished by the physical/link protocol(s) running immediately below the network layer. Possible values are Ethernet-CSMACD (for Ethernet, Fast Ethernet, and Gigabit Ethernet) and Other (VLAN).

RMON Ethernet statistics are displayed in four groups:

Counts
Bytes	Displays the total number of bytes contained in packets processed on the network segment including bytes contained in error packets.
Packets	Displays the total number of packets processed on the network segment including error packets.
Drop Events	This field indicates the number of times packets were dropped because the device could not keep up with the flow of traffic on the network. Note that this value does not reflect the number of packets dropped, but only the number of times packets were dropped.

Packet Type
Multicast	Indicates the number of good packets processed on the network segment that were destined for more than one address. Note that this total does not include broadcast packets.
Broadcast	Indicates the number of good packets processed on the network segment that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.
Unicast	Indicates the number of good packets processed on the network segment that were destined for a single address.

The percentages displayed to the right of the numerical values for these fields indicate what percentage of good packets transmitted on the network segment were multicast, broadcast, and unicast; these percentages will add up to 100. The pie chart provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes.

Packets

The Frame Size (Bytes) Pkts fields indicate the number of packets (including error packets) processed by the network segment that were of the noted length, excluding framing bits but including frame check sequence bits. Packet sizes counted are:

- 64
- 65-127
- 128-255
- 256-511
- 512-1023
- 1024-1518

The percentages displayed to the right of the numerical values for these fields indicate what percentage of all packets transmitted on the network segment were of the noted size. Unless the network segment has experienced a significant number of runts and/or giants (which are not counted in this group), these percentages will add up to 100. The pie chart provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes.

Errors

CRC/Alignment
Indicates the number of packets processed by the network segment that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check, or CRC error).

Fragments
Indicates the number of packets processed by the network segment that were undersized (less than 64 bytes in length; a runt packet) *and* had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

Jabbers
Indicates the number of packets processed by the network segment that were oversized (greater than 1518 bytes; a giant packet) *and* had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

Collisions
Indicates the total number of **receive** (those the device detects while receiving a transmission) and **transmit** (those the device detects while transmitting) collisions detected on the network segment.

Undersized
Indicates the number of packets processed by the network segment that contained fewer than 64 bytes (runt packets) but were otherwise well-formed.

Oversized   Indicates the number of packets processed by the network segment that contained more than 1518 bytes (giant packets) but were otherwise well-formed.

The percentages displayed to the right of the numerical values for these fields indicate what percentage of **total packets** transmitted on the network segment were of the noted type. The percentage field for Collisions will always display N/A because collisions are not true errors; percentages are not calculated, and will not be represented in the pie chart. The pie chart provides a graphical view of the selected percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes.

Viewing Total, Delta, and Accumulated Statistics

Use the Calculation Mode drop-down list located at the bottom of the window to specify how the statistics count will be calculated:

Poll   After the completion of the current polling cycle plus one complete polling cycle, the window will display the total count of statistics processed since the device was last initialized. These totals are updated after each polling cycle.

Delta   After the completion of the current polling cycle plus two more polling cycles, the window will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.

Accumulate   After the completion of the current polling cycle plus two more polling cycles, the window will display a fresh cumulative count of statistics. This option does not clear the device counters; you can still re-select Poll for the total count since the device was last initialized.

TIP
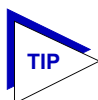
The RMON Ethernet Statistics window uses the polling intervals you have set via the Poll Settings window. See Poll Settings in Chapter 2, for more information.

Interface Statistics

The Interface Statistics window (Figure 3-2) provides color-coded statistical information about each individual bridge port on your device. The first four statistics are graphically displayed in color-coded form in the pie chart. These statistics are updated with each poll to the device.

To open the Interface Statistics window:

1. Click on the desired **port number** in the Device View. The Port menu will appear.

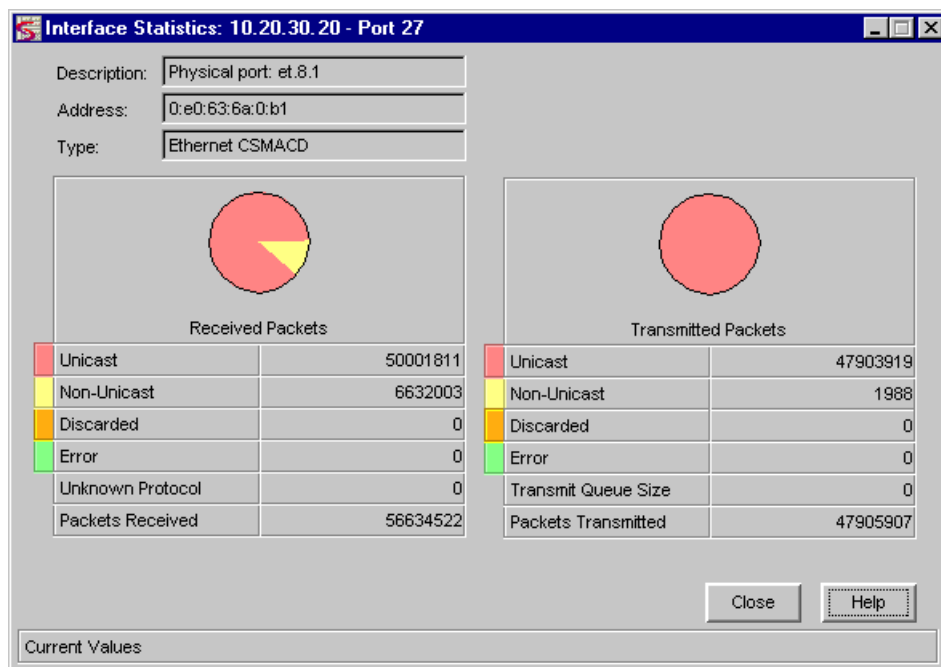2. Select **Interface Statistics**. The Interface Statistics (Figure 3-2) window opens.

Figure 3-2. Interface Statistics window

> **TIP**
>
> *You can also access this window by selecting the desired interface in the Interface Summary window, and clicking the **Statistics** button.*

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

Description
Displays a description of the port and the type of interface followed by the board and port number.

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

Type
The type of interface, distinguished by the physical/link protocol(s) running immediately below the network layer. Possible values are Ethernet-CSMACD (for Ethernet, Fast Ethernet, and Gigabit Ethernet) and Other (VLAN).

The lower portion of the window provides the following transmit and receive statistics, with the first four statistics 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.

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.

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 reconfigure your bridging parameters, or perhaps reconfigure your network to add additional bridges or switches. Consult the Enterasys *Network Troubleshooting Guide* for more information.

Error
Displays the number of packets received or transmitted that contained errors.

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 total 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 device begins to discard packets.

Packets Transmitted *(Transmit only)*
Displays the total number of packets transmitted by this 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

Utilities

TFTP Download and Configuration File Upload/Download

NetSight Element Manager provides two file transfer utilities for the X-Pedition Router: TFTP Download and Configuration Upload/Download. TFTP Download lets you download a new firmware image to your router. Configuration Upload/Download lets you upload and download the router's Configuration file using TFTP.

You must have a TFTP Server running on your machine to perform these transfer operations. On the Windows® Platform, you must have the Remote Administration Tools application running to provide the TFTP server. (Refer to your Remote Administration Tools User's Guide for more information.) On the UNIX® Solaris® Platform, you must configure a TFTP Server to operate on your machine.

TFTP Download

The TFTP Download window (Figure 4-1) allows you to access a firmware image file available anywhere on your network and initiate a download of the file to a router.

To open the TFTP Download window:

1. Click on **Utilities** in the Device View menu bar. The Utilities menu will appear.

2. Select **TFTP Download**. The TFTP Download (Figure 4-1) window opens.
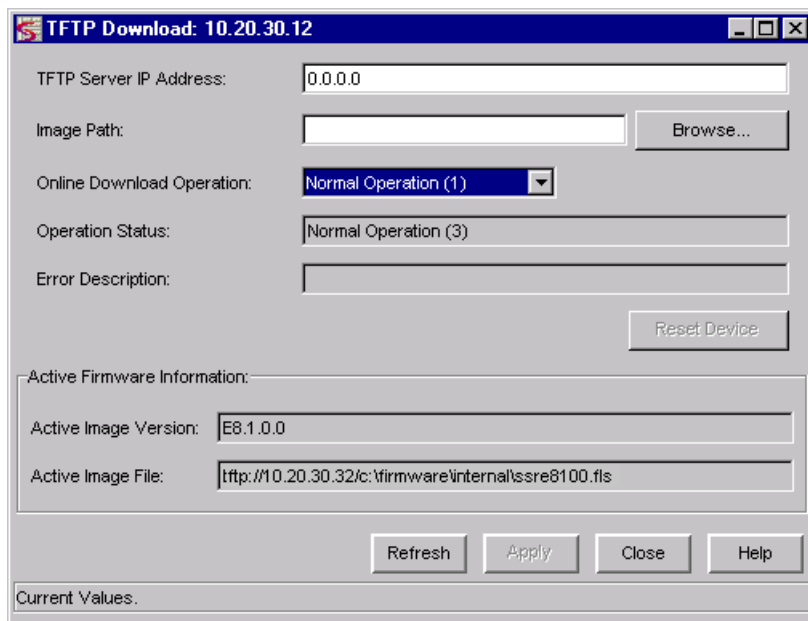
Figure 4-1. The TFTP Download Window

The TFTP Download window allows you to configure and perform a download operation, and view status and error information regarding the download.

You can view information about the firmware image currently active in the router in the Active Firmware Information area:

Active Image Version
This field displays the version of firmware currently active the device.

Active Image File
Displays the location and filename of the active firmware image.

Performing a Download

Use the fields in the top part of the TFTP Download window to configure your download:

1. In the **TFTP Server IP Address** field, enter the IP address for the TFTP Server.

2. In the **Image Path** field, enter the path and filename of the image file you want to download, or use the Browse button to navigate to the file.

3. In the **Online Download Operation** field, use the drop-down list to select the type of download operation you want to perform:

    •   **Normal Operation** -- the device is in normal operation.

- **Download File** -- perform an online download.

- **Download File and Reset** -- perform an online download and reboot with the new image as soon as the download is complete.

4. Click **Apply** to begin the download.

The Operation Status field displays the status of the download operation:

- Normal Operation -- either a download was performed with no reset specified, or no download has been started.

- Download Active -- a download has started.

- Error Detected During Download -- A download was started but an error was detected.

The Error Description field displays a description of any error detected during a download.

Configuration Upload/Download

The X-Pedition Router has a Configuration file that contains information such as interface, RMON, VLAN, and Spanning Tree configuration for the device. Use this window to upload and download this file to and from the device using TFTP. You can use these procedures as a way to backup the Configuration file, or copy the Configuration file from one router to another.

To open the Configuration Upload/Download window:

1. Click on **Utilities** in the Device View menu bar. The Utilities menu will appear.

2. Select **Config Upload/Download**. The Configuration Upload/Download (Figure 4-2) window opens.
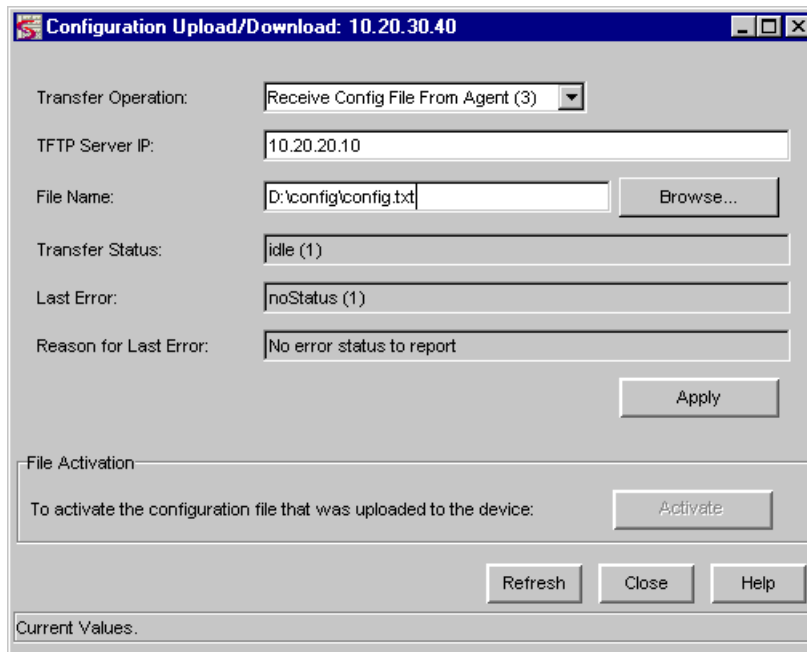
Figure 4-2. Configuration Upload/Download window

Performing an Upload or Download

Use the fields in the top part of the Configuration Upload/Download window to configure your upload or download:

1. In the Transfer Operation field, use the drop-down list to select the type of transfer operation you want to perform. (The term "Agent" refers to the router.)

   • **No Operation** -- no transfer is taking place

   • **Send Config File to Agent** -- the Configuration file will be uploaded to the router.

   • **Receive Config File from Agent** -- the Configuration file will be download from the router.

   • **Receive Bootlog File from Agent** -- the Bootlog file will be downloaded from the router.

1. In the **TFTP Server IP** field, enter the IP address for the TFTP Server.

2. In the **File Name** field, enter the path and filename of the Configuration file you want to upload/download, or use the **Browse** button to navigate to the file. Whether or not you should specify an existing file depends on whether you have installed NetSight Element Manager on the Windows or Solaris Platform.

- • **Windows Platform** -- you cannot specify an existing file. The transfer operation will create a new file with the filename you have specified.

- • **Solaris Platform** -- you must specify an existing file. The transfer operation will not create a new file. Any information in the existing file will be overwritten.

3. Click **Apply** to perform the upload or download operation.

4. If you have performed an upload of a Configuration file, once the upload is complete, click **Activate** to activate the Configuration file that was uploaded to the router.

The Transfer Status field displays the status of the upload or download operation:

- • idle -- no transfer is taking place.

- • sending -- the file is being downloaded from the router.

- • receiving -- the file is being uploaded to the router.

- • transfer complete -- the transfer has completed successfully.

- • error -- the transfer has failed.

The Last Error field displays the last error message received during a failed transfer operation, and the Reason for Last Error field displays additional information on the Last Error.

Index

Numerics