FN 100 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 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: 9031897-03 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.

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 FN100 Chassis View

Chapter 3 FN100 Virtual Switching

Chapter 1

Introduction

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

Welcome to the ***FN100™ User's Guide***. We have designed this guide to serve as a simple reference for using NetSight Element Manager for the FN100.

As a part of the Fast Network product line of switches, the FN100 provides a foundation for high speed scalable Ethernet switching solutions. The FN100 is a high performance, intelligent Fast Ethernet switch designed to support full 10 Mbps or 100 Mbps connectivity on 8 or 16 ports over unshielded twisted-pair (UTP) and / or multimode (MM) fiber. The FN100 consists of 8 or 16 10 / 100Base-TX or 10 / 100Base FX ports and, in the case of the TX models, 1 or 2 selectable 100Base-FX ports. The FN100 is IEEE 802.2, 802.3 and 802.1d compliant, includes built-in SNMP management, and supports MIB II, PPP, and Enterprise MIB.

Using the FN100 User's Guide

Each chapter in this guide describes one major functionality or a collection of several smaller functionalities of the FN100 device module. This guide contains information about software functions which are accessed directly from the device icon.

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

Chapter 2, **The FN100 Chassis View**, describes the visual display of the FN100-switch and explains how to use the mouse within the Chassis View; the operation of chassis-level management functions — like enabling and disabling ports — is also described here.

Chapter 3, **FN100 Virtual Switching**, describes using the FN100 Virtual Switching window to refine your network and control bandwidth usage by assigning the FN100's ports to any of four available virtual switches.

Chapter 4, **Using FN100 Trunking**, details using the FN100 Port Trunking window to create trunk groups, allowing you to increase aggregate bandwidth when two or more switches are connected.

Chapter 5, **Workgroup Configuration**, describes configuring work groups by specifying a subset of device ports and the type(s) of packets (multicast, unicast, or both) that are to be forwarded by those ports, thereby allowing you to restrict multicast traffic from being propagated through every bridge port on your device.

Related Manuals

The ***FN100 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 FN100 include:

User's Guide

Tools Guide

Remote Administration Tools User's Guide

Remote Monitoring (RMON) User's Guide

Alarm and Event Handling User's Guide

For more information about the capabilities of the FN100, consult the appropriate hardware documentation.

Software Conventions

NetSight Element Manager's device 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.

Common FN100 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 1-1.

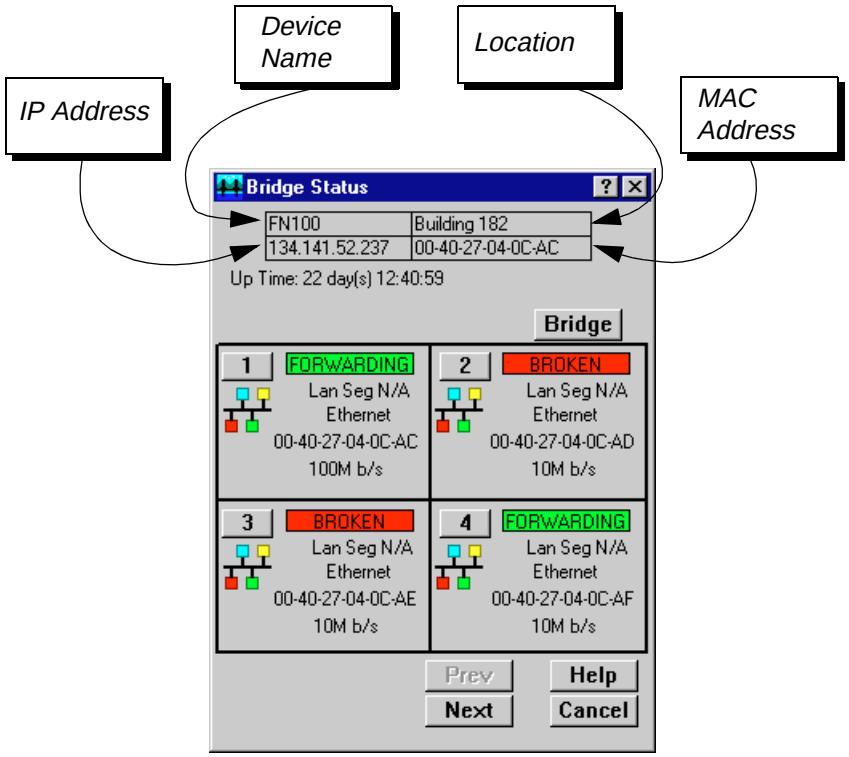


Figure 1-1. Sample Window Showing Informational Text Boxes

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 FN100; 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 associated with the IP Address used to define the device icon when it was added to NetSight Element Manager. 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:

Port Number
Displays the number of the monitored port.

Uptime
Displays the amount of time, in a X days hh:mm:ss format, that the FN100 has been running since the last start-up.

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:

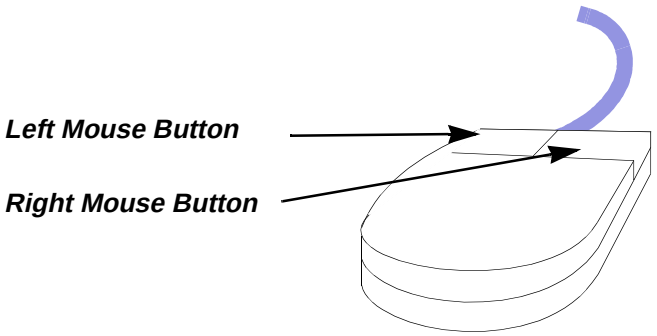


Figure 1-2. Mouse Buttons

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.

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.

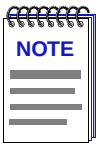
Getting Help

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 FN100 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. 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.



All of the on-line 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.*

Getting Help from the Global Technical Assistance Center

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

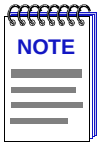
By phone:	(603) 332-9400 *24 hours a day, 365 days a year*
By fax:	(603) 337-3075
By mail:	Enterasys Networks PO Box 5005 Rochester, NH 03866-5005
By e-mail:	support@enterasys.com
FTP:	ftp.ctron.com (134.141.197.25)
Login	`anonymous`
Password	`your e-mail address`
By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

Send your questions, comments, and suggestions regarding NetSight Element Manager 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/



*For the highest firmware versions successfully tested with NetSight Element Manager 2.2.1, refer to the **Readme** file available from the NetSight Element Manager 2.2.1 program group. If you have an earlier version of firmware and experience problems, contact Technical Support for upgrade information.*

Chapter 2

The FN100 Chassis View

About the Chassis View window; the Chassis Manager window; Hub management functions

The FN100 Chassis View window is the main screen that immediately informs you of the current condition of individual ports on your switch via a graphical display. The Chassis View window also serves as a single point of access to all other FN100 windows and screens, which are discussed at length in the following chapters.

To access the FN100 Chassis View window, use one of the following options:

1. In any map, list, or tree view, double-click on the FN100 you wish to manage;

   or

1. In any map, list, or tree view, click the **left** mouse button once to select the FN100 device you wish to manage.
2. Select **Manage—>Node** from the main NetSight Element Manager 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 FN100 device you wish to manage.
2. On the resulting menu, click to select **Manage**.

Viewing Chassis Information

The FN100 Chassis View window (Figure 2-1) provides a graphic representation of the FN100, including a color-coded port display which immediately informs you of the current configuration and status of the switch and its ports.

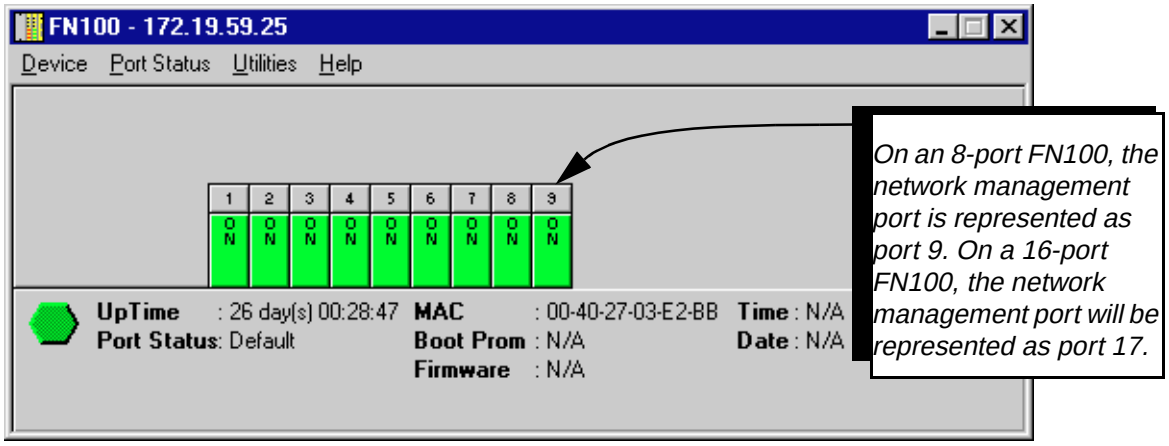


Figure 2-1. FN100 Chassis View Window

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- 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.

Front Panel Information

The areas above and below the main port display area provide the following device information:

IP

The Internet Protocol address assigned to the FN100 appears in the title bar of the Chassis View window; this field will display the IP address you have used to create the FN100 icon. IP addresses are assigned via Local Management.

Connection Status

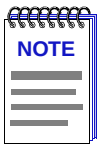
This color-coded area indicates the current state of communication between NetSight Element Manager and the FN100.

- **Green** indicates the FN100 is responding to device polls (valid connection).
- **Magenta** indicates that the FN100 is in a temporary stand-by mode while it responds to a physical change in the hub; note that port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status – polling has not yet been established with the FN100.
- **Red** indicates the FN100 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 day(s) hh:mm:ss format, that the FN100 has been running since the last start-up.

Port Status
If management for your device supports a variable port display (detailed in **The FN100 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 interface associated with the IP Address used to define the device icon when it was added to NetSight Element Manager. MAC addresses are factory-set cannot be altered.



Boot Prom, Firmware, Time, and Date, are not available for the FN100 at the time of this release.

Boot Prom
The revision of BOOT PROM installed in the FN100.

Firmware
The revision of device firmware stored in the FN100's FLASH PROMs.

Time
The current time, in a 24-hour hh:mm:ss format, set in the FN100's internal clock.

Date
The current date, in an mm / dd / yy format, set in the FN100's internal clock.

Menu Structure

By clicking on various areas of the FN100 Chassis View display, you can access menus with device- 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:

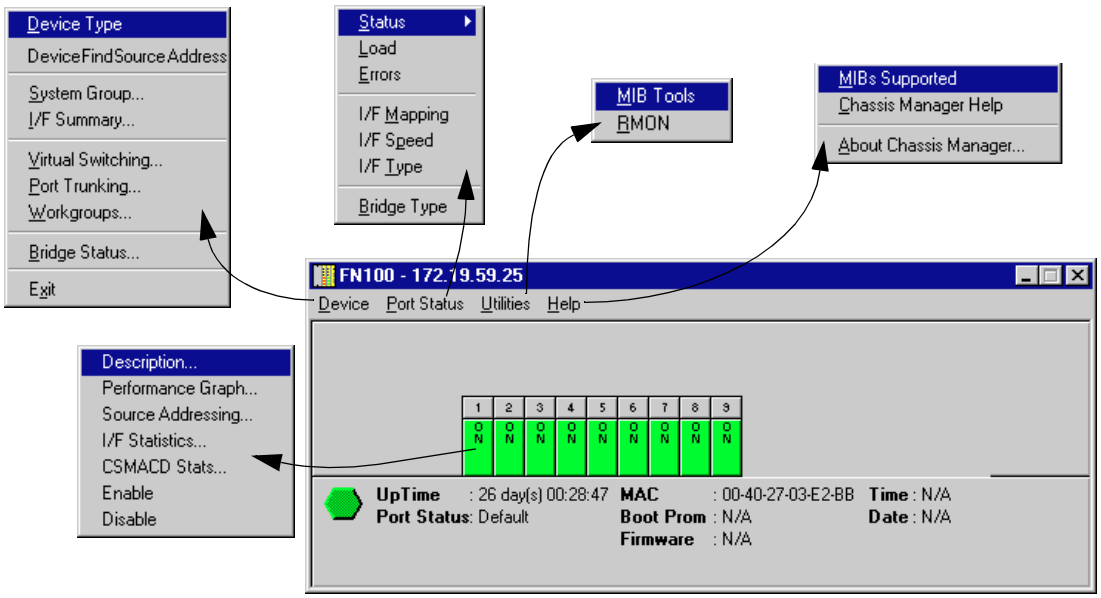


Figure 2-2. FN100 Chassis View Menu Structure

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. See **Viewing the Device Type** for details.
- **Device Find Source Address**, enables you to determine through which interface a specified MAC address is communicating by searching the 802.1d bridge Filtering database. Ethernet MicroLAN switches will also search the repeater Source Address Table (SAT). If the specified MAC address is located, a list of interface(s) through which the given address is communicating will be displayed.
- **System Group...**, which allows you to manage the FN100 via SNMP MIB II. Refer to the ***Generic SNMP User's Guide*** for further information.
- **I/F Summary**, which allows you to view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your FN-10. See **Viewing I/F Summary Information** on page 2-13 for more information.

- **Virtual Switching...**, which launches the FN100 Virtual Switching window, allowing you to refine your network and control bandwidth usage by assigning the FN100's ports to any of four available virtual switches. See Chapter 3, **FN100 Virtual Switching**, for details.
- **Port Trunking...**, which allows you to use the FN100 Port Trunking window to create trunk groups, letting you increase aggregate bandwidth when two or more switches are connected. See Chapter 4, **Using FN100 Trunking**, for details.
- **Workgroups...**, which invokes a window that lets you configure work groups by specifying a subset of device ports and the type(s) of packets (multicast, unicast, or both) that are to be forwarded by those ports, thereby allowing you to restrict multicast traffic from being propagated through every bridge port on your device. See Chapter 5, **Workgroup Configuration**, for details.
- **Bridge Status...**, which opens a window that provides an overview of bridging information for each interface, and allows you to access all other bridge-related options. Refer to the bridging chapter in the ***Tools Guide*** for details.
- **Exit**, which closes the FN100 Chassis View window.

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 Chassis View window:

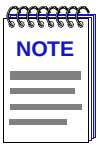
- **Status** allows you to select one of three status type displays: Bridge, Admin, or Operator.
- **Load** will display the portion of network load processed per polling interval by each interface as a percentage of the theoretical maximum load (10 or 100 Mbits / sec).
- **Errors** allows you to display the number of errors detected per polling interval by each interface as a percentage of the total number of valid packets processed by the interface.
- **I/F Mapping** will display the interface (if) index associated with each port on your FN100 switch.
- **I/F Speed** will display the speed (100 Mbits / sec) of the network segment attached to each port. The speed of the network management port will be displayed in Kbits / sec.
- **I/F Type** will display the interface type of each port in the FN100 — i.e., Eth (ethernet-csmacd) for the bridging interfaces, and PPP for the network management port.
- **Bridge Type** refers to the type of bridging in effect, which will always be **TP** (transparent) on an FN100.

For more information on the port display options available via this menu, see **The FN100 Port Status Displays**, later in this chapter.

The Utilities Menu

From the **Utilities** menu you can select:

- **MIB Tools**, provides direct access to the FN100's MIB information. This selection is also available from the **Tools** menu at the top of the NetSight Element Manager's main window. Refer to the ***Tools Guide*** for more information on the MIB Tools utility.
- **RMON**, for launching the Remote Network Monitoring application. RMON is described in its own ***User's Guide***. Like MIB Tools, RMON can also be launched from the **Tools** menu.



*Using the MIBTools utility, you will have access to MIB information for FN100 interfaces that are assigned to the default virtual switch. MIB information for interfaces assigned to a virtual switch other than the default virtual switch will be unavailable via MIBTools. See Chapter 3, **FN100 Virtual Switching**, for details on viewing and changing the default virtual switch setting.*

The Help Menu

The Help Menu has two selections:

- **Mibs Supported**, which brings up the Chassis Manager window. See **The Chassis Manager Window**, later in this chapter, for details.
- **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 for the Chassis Manager application in use.

The Port Menus

The menu for bridging ports offers the following selections:

- **Description...**, which brings up a window describing the selected port; see **Viewing the Port Description**, later in this chapter.
- **Performance Graph...**, which allows you to view the traffic going through a selected bridge. This information is displayed both numerically and graphically, as described in your ***Tools Guide*** bridging chapter.
- **Source Addressing...**, which displays a list of MAC Addresses that communicate through the selected bridge port.
- **I/F Statistics...**, which allows you to view color-coded statistical information about the selected bridge port; see **Viewing Interface Detail** later in this chapter.
- **CSMACD Stats...**, which graphically displays Receive, Transmission, and Collision errors over the selected bridge port; see **Viewing CSMACD Statistics** later in this chapter.

- **Enable/Disable**, which administratively turns the selected bridging port on or off; see **Viewing I/F Summary Information** on page 2-13 for more information.

The FN100 Port Status Displays

When you open the Chassis View window, each port on the FN100 will display its Admin 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 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:

Status

You can view four status categories for your ports:

- **Bridge** — FWD (forwarding), DIS (disabled), LIS (listening), LRN (learning), BLK (blocking), BRK (broken), or UNK (unknown).
- **Bridge Mapping** — bridge interface index numbers
- **Admin** — ON or OFF
- **Operator** — ON or OFF

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

- FWD (forwarding) when the interface is on-line and forwarding packets from one network segment to another.
- DIS (disabled) when bridging at the interface has been disabled by management, and no traffic can be received or forwarded on this interface.
- LIS (listening) when the interface is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
- LRN (learning) when the Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change.
- BLK (blocking) when the interface is on-line, but filtering traffic from going across the FN100 from one network segment to another.

- BRK (broken) when the physical interface has malfunctioned.
- UNK (unknown) if the interface's status cannot be determined.

If you have selected **Bridge Mapping**, the port status boxes will display the *bridge* interface index numbers assigned to each interface (which may or may not match the *ifIndex* values displayed via the **I/F Mapping** option described below).

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

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

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

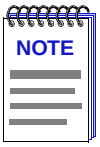
- ON if the port is actively forwarding and receiving packets.
- OFF if the port is not currently forwarding and receiving packets.

Load

If you choose **Load**, the interface 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 per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits / sec) of an Ethernet network.

Errors

If you choose the **Errors** mode, the interface boxes will 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.



*The polling interval is set via the **Tools —> Options...—>Polling** option from the main window's menu bar. Refer to the **User's Guide** for full information on setting device polling intervals.*

I/F Mapping

If you choose the **I/F Mapping** mode, each port text box will display its MIB II ifIndex value.

I/F Speed

If you choose the **I/F Speed** mode, the port text boxes will display the speed (100 Mbits / sec) of the network segment connected to each port. The speed of the network management port will be displayed in Kbits / sec.

I/F Type

If you choose the **I/F Type** mode, the port text boxes will display the port type (e.g., Eth, PPP) of each port, as determined by the port's MIB II ifType value.

Port Status Color Codes

The **Bridge** port display mode incorporates the following color-coding scheme: green = FWD, blue = DIS, magenta = LIS/LRN, orange = BLK, red = BRK, and gray = UNK.

The **Admin** and **Operator** port display modes use the following color-coding scheme: green = ON, red = OFF.

For the **Load**, **Errors**, **I/F Mapping**, **I/F Speed**, and **I/F Type** port display modes, color codes will continue to reflect the most recently selected mode which incorporates its own color coding scheme.

The Chassis Manager Window

The FN100 draws its functionality from a collection of proprietary MIBs and IETF RFCs, and organizes its MIB data into a series of components. A MIB component is a logical grouping of MIB data; each group controls a defined set of objects. For example, FN100 bridging information is organized into its own component. Note, too, that there is no one-to-one correspondence between MIBs and MIB components; a single MIB component might contain objects from several different proprietary MIBs and RFCs.

The Chassis Manager window, Figure 2-3, 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.

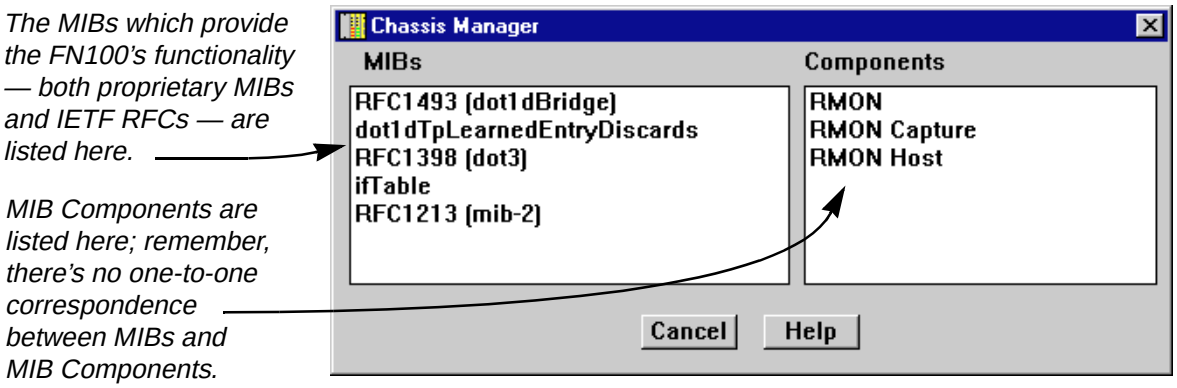


Figure 2-3. Chassis Manager Window

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 the FN100 and its ports.

Viewing the Device Type

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

Figure 2-4. Device Type Window

Viewing the Port Description

Choosing the **Description...** option on the individual port interface menus brings up a window that describes that interface you have selected. Depending on the type of port you select, one of the following windows will appear:

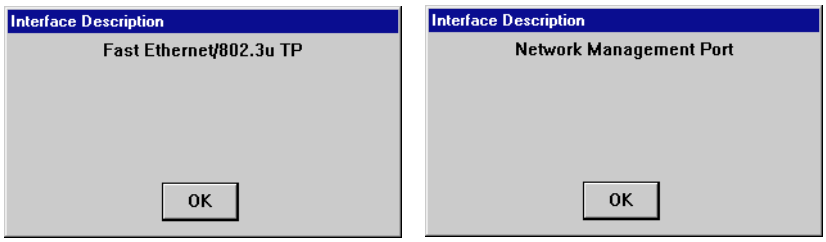


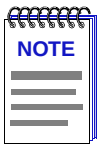
Figure 2-5. Port Description Windows

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 available to configure your device and keep it operating properly. Hub management for the FN100 is comprised of locating source addresses, viewing interface statistics and CSMACD statistics, as well as administratively enabling and disabling the ports.

Using Device Find Source Address

When you select the **Device 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.



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 Device Find Source Address window:

1. Click on **Device** in the Chassis View menu bar.
2. Click on **Device Find Source Address**. The Device Find Source Address window, as shown in Figure 2-6, opens.

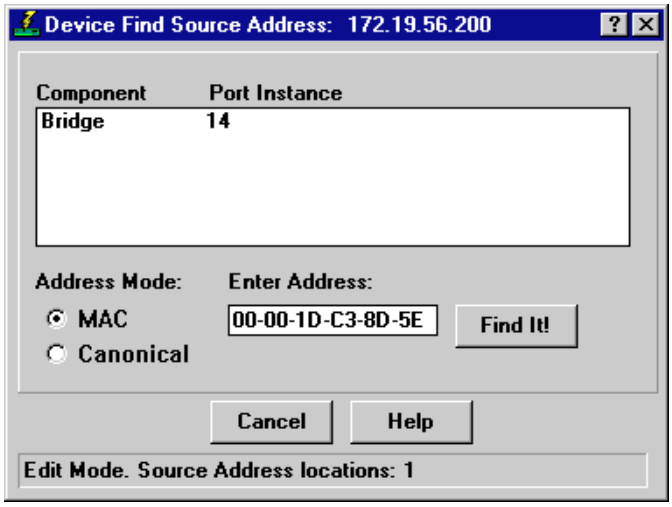


Figure 2-6. Device Find Source Address Window

The Device 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.

To use the Device Find Source Address window:

1. In the **Address Mode** field, select the format of the Source Address you wish to find, either **MAC** or **Canonical**.
2. In the **Enter Address** text box, enter the Source Address you wish to find in the appropriate XX-XX-XX-XX-XX-XX format.

NOTE

*If you enter the MAC format of a specified address, and then click on **Canonical**, NetSight Element Manager will do the address conversion for you, from the Ethernet hexadecimal format to the Token Ring Canonical format. The same is also true if you enter the Canonical format of a specified address and then select **MAC**.*

3. Click on the **Find It!** button. A "**Processing Request**" message opens in the status bar at the bottom of the window.

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

NOTE

*If the MAC address is entered in an incorrect format, an "**Invalid MAC Address. Enter Valid MAC Address**" message displays. Enter the address in the correct XX-XX-XX-XX-XX-XX hexadecimal format.*

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 2-7, will appear.

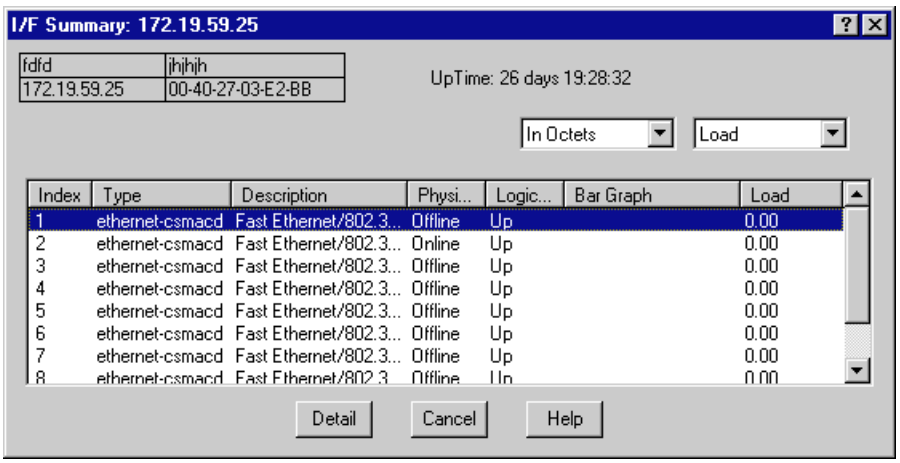


Figure 2-7. I/F Summary Window

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. Possible values are ethernet-csmacd (for both standard and Fast Ethernet front panel interfaces) and PPP.

Description
A text description of the interface: Ethernet, Fast Ethernet, or Network Management Port.

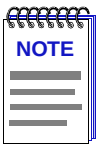
Physical Status
Displays the current physical status — or operational state — of the interface: **Online** or **Offline**.

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**.



*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 of the network to which the device is connected (100 Mbps for Fast 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 2-8) provides detailed MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for each individual port interface. 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 will appear.

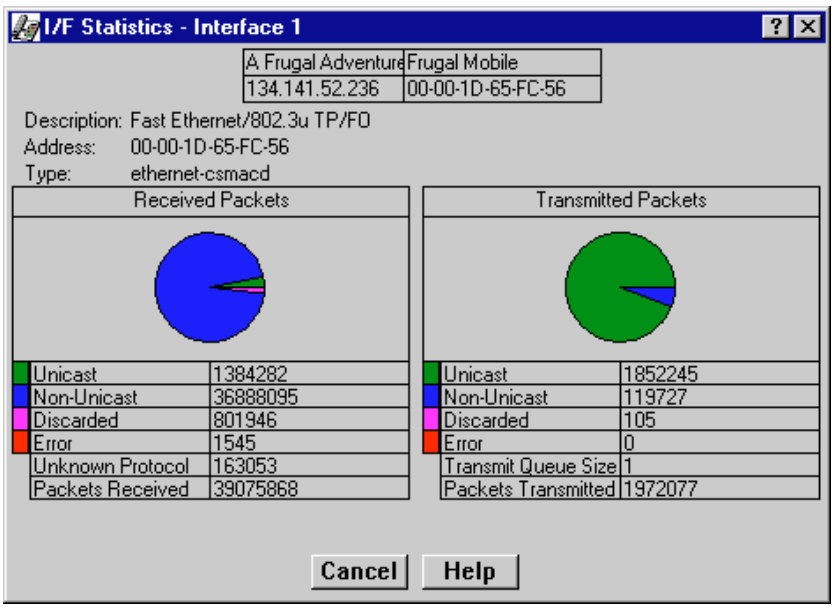


Figure 2-8. Detail Interface Statistics

You can also access this information via the I/F Statistics option available on the individual port menus.

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

Description
Displays the interface description for the currently selected interface: Ethernet or Fast 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 FN100 will begin to discard packets.

Packets Transmitted *(Transmit only)*
Displays the 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:

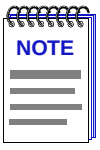
`Received Discards + Transmitted Discards`

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



*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 information on the System Group and Interface Group windows.*

Viewing CSMACD Statistics

The CSCMACD Statistics Windows display statistics for each bridging interface on your FN100. Receive errors, transmission errors, and collision errors are displayed in this window.

Three color-coded pie charts allow you to view the breakdowns of each statistics group.

To access the CSMACD Statistics window from the Chassis View window:

1. Click on the desired port to reveal the Port menu.
2. Choose **CSMACD Stats...**. The following window will appear (Figure 2-9).

NOTE

The CSMACD Statistics window can also be accessed from the Bridge Status window. See the bridging chapter in the **Tools Guide** *for more information.*

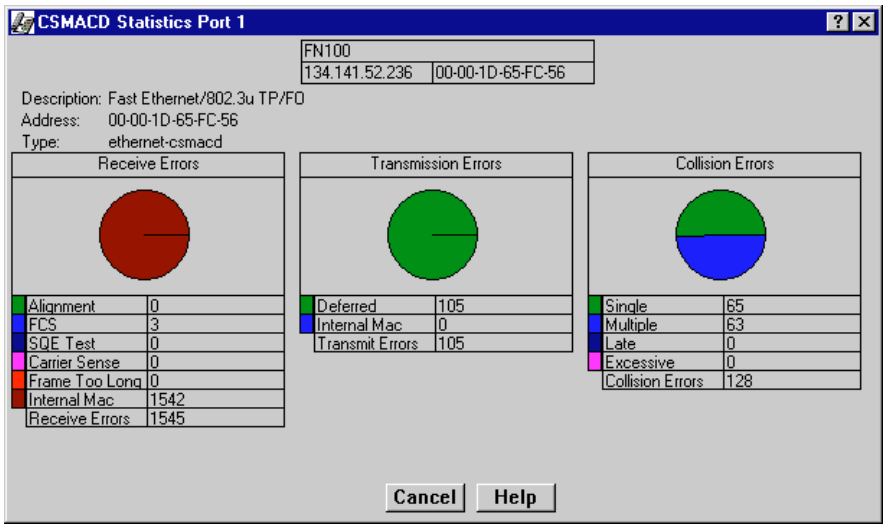


Figure 2-9. CSMACD Statistics Window

Each of the receive, transmission, and collision errors is described below.

Receive Errors

Alignment
The number of frames received on a particular interface that contain a non-integral number of bytes (color-coded green). Misaligned packets can result from

a MAC layer packet formation problem, or from a cabling problem that is corrupting or losing data.

FCS

The number of frames received on a particular interface that are an integral number of bytes in length, but do not pass the FCS (Frame Check Sequence) check. FCS, or Frame Check Sequence, errors occur when packets are somehow damaged on transit. When each packet is transmitted, the transmitting interface computes a frame check sequence (FCS) value based on the contents of the packet, and appends that value to the packet. The receiving interface performs the same computation; if the FCS values differ, the packet is assumed to have been corrupted and is counted as an FCS error.

SQE Test

Displays the number of times that the SQE Test Error message is generated by the PLS sublayer on the selected interface. The SQE (Signal Quality Error) Test tests the collision detect circuitry after each transmission. If the SQE Test fails, a SQE Test Error is sent to the interface to indicate that the collision detect circuitry is malfunctioning.

Carrier Sense

Displays the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. Carrier sense describes the action an interface desiring to transmit will take to listen to the communication channel to see if any other interface is transmitting. If a “carrier is sensed,” the sensing interface will wait a random length of time, and then attempt to transmit.

Frame Too Long

Displays the amount of frames received on this interface that exceed the maximum permitted frame size.

Internal MAC

The number of frames that failed to be received by the interface due to an internal MAC sublayer receive error. These errors are only counted if a Frame Too Long, Alignment, or FCS Error did not occur along with the internal MAC error.

Receive Errors

Displays the total number of receive errors of all types that were detected by the selected interface while it was receiving a transmission.

Transmission Errors

Deferred

Displays the number of frames for which the first transmission attempt on this interface is delayed because the medium is busy.

Internal MAC
The number of frames for which transmission fails due to an internal MAC sublayer transmit error. This error is only counted in this window if there have not been corresponding Late Collisions, Excessive Collisions, or Carrier Sense Errors.

Transmit Errors
The total of transmission errors of all types that occurred while the selected interface was attempting to transmit frames.

Collision Errors

Single
Displays the number of successfully transmitted frames on the selected interface for which transmission was prevented by **one** collision.

Multiple
Displays the number of successfully transmitted frames on the selected interface for which transmission was prevented by **more than one** collision.

Late
Displays the number of times that a collision has been detected on this interface later than 51.2 microseconds into the transmission of the packet on a 10 Mbit/s system or later than 5.12 microseconds on a 100 Mbit/s system.

Excessive
Displays the number of frames from this interface for which transmission was not complete due to excessive collisions.

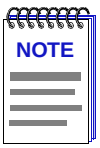
Collision Errors
Displays the total number of collision errors of all types that occurred during transmission from this interface.

Enabling and Disabling Ports

From the Port menus on the FN100 Chassis View window, you can administratively enable and disable the ports. When you administratively disable a bridge port, 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 a port, the port moves from the Disabled state, through the Learning and Listening states, to the Forwarding state; bridge port state color codes will change accordingly.

To enable or disable a bridge port:

1. Click on the desired Port index. The Port menu will appear.
2. Click on **Enable** to enable the port, or **Disable** to disable the port. You will get a confirmation window asking if you're "sure you want to Enable/Disable this Bridge Port." Click **OK** and your port will now be enabled or disabled.



For more information about bridging functions and how to determine the current state of each bridge port, see the bridging chapter in the **Tools Guide**.

Chapter 3

FN100 Virtual Switching

FN100 virtual switches; performing virtual switching

The FN100 Virtual Switching window (Figure 3-1) allows you to refine your network and control bandwidth usage by assigning the FN100's ports to any of four available virtual switches. This feature can be used to logically group network users and control the amount and type of traffic that is propagated beyond each logical group.

Using this window, you can configure up to four logical segments that can include multiple physical segments attached to the front panel ports (e.g., physical segments inserted in ports 1, 2, 5, and 8 could all be assigned to Switch 3, and would communicate as if they actually were on the same physical segment). Using this capability, 10 and 100 Mbps devices can be placed on separate physical segments, allowing the 100 Mbps devices to operate at full speed, and the switch can treat both segments as a single logical network.

Each virtual switch is assigned a unique bridge ID and is treated as a separate bridge by Spanning Tree. The bridge ID for each virtual switch is based on the MAC address of the port in each group with the lowest index number.

The Default Switch setting determines which of the four available virtual switches is queried for port-specific information for the Spanning Tree protocol. Because each virtual switch is treated as a separate bridge by Spanning Tree, only ports which are assigned to the Default Switch will be recognized by Spanning Tree and correctly represented in the Bridge Status window.

Performing Virtual Switching

To launch the FN100 Virtual Switching window from the FN100 Chassis View:

1. Click to display the **Device** menu.
2. Drag down to **Virtual Switching...**, and release. The Virtual Switching window (Figure 3-1) will appear.

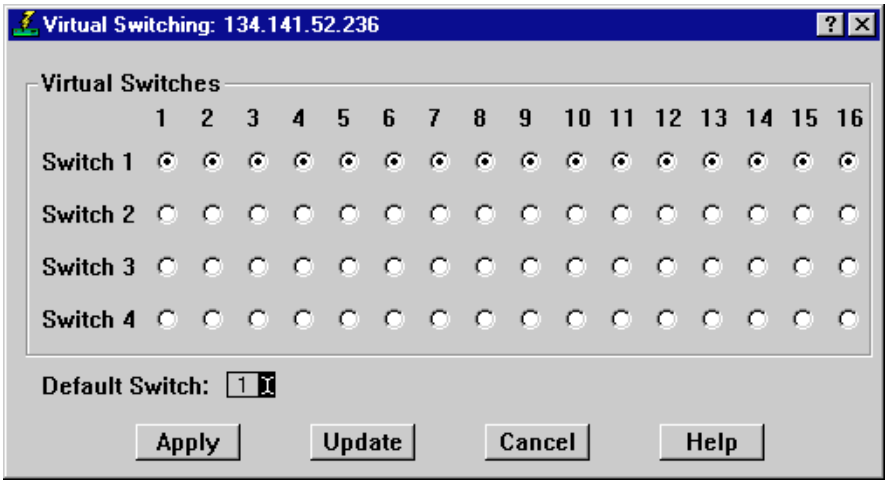


Figure 3-1. The Virtual Switching Window

The Virtual Switching window features a column of four radio buttons (one button for each virtual switch) for each of the FN100's ports. The port indices are listed atop each column.

The Virtual Switching window also features:

Update
When the **Update** button is clicked, the FN100 will be queried for its virtual switch settings, and any changes that have occurred since the window was opened (or since the **Update** button was last clicked) will be reflected in the window.

Configuring Your Virtual Switch Settings

To assign the FN100's ports to any of the four virtual switches:

1. For each port that you wish to assign to a virtual switch, click on the port's radio button (in the column beneath the port's index number) that corresponds to the desired switch setting.
2. Click **Apply**. The Virtual Switching window will update to reflect the new configuration.

NOTE

If you use the Virtual Switching window to assign ports to a virtual switch other than the one defined as the default switch, those ports will not be correctly represented in the Bridge Status window. This is because each virtual switch has a separate bridge ID and is treated as a separate bridge by Spanning Tree. To correctly view these ports in the Bridge Status window, you must change the default virtual switch setting using the ***Default Switch*** *field.*

Defining a Default Switch

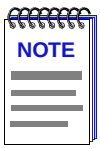
By defining a default switch setting, you decide which of the FN100's four virtual switches will be recognized by Spanning Tree and reflected in the FN100 Bridge Status window. When you change the default switch, only those ports which are assigned to the selected default switch will be correctly displayed in the Bridge Status window. All other ports will return an UNKNOWN bridge state.

To define a default switch for your FN100:

1. Click the I-bar cursor (I) next to the **Default Switch:** field near the bottom of the Virtual Switching window. The Change Default Switch window will appear.

Figure 3-2. The Change Default Switch Window

2. Enter the desired default switch number. Allowable entries are 1, 2, 3, or 4.
3. Click **OK** to select the default switch you have entered. Click **Cancel** to exit the window without making any changes.



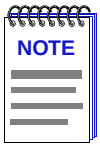
When the FN100 is reset, all ports will revert to Virtual Switch #1. The Default Switch will also revert to 1.

Chapter 4

Using FN100 Trunking

The Trunking Table window; enabling and disabling trunking

Trunking, an extension of the 802.1D Spanning Tree protocol, allows you to increase aggregate bandwidth when two or more switches are connected. A single 10/100BASE-T connection between switches yields 10 or 100 Mbps of bandwidth, depending on the speed of the ports used for the connection. A trunk group is created when two or more ports on the same switch (for which trunking protocol is enabled) are physically connected to the same remote switch. By creating a trunk group, each additional connection results in another 10 or 100 Mbps of bandwidth, since the group of ports effectively acts as a single connection. The trunking protocol modifies Spanning Tree to allow the redundant links which form a trunk group. Trunking can be enabled or disabled for a port using the Trunking Table window (Figure 4-1). Trunking can be enabled for use on up to eight ports per switch, allowing you to configure up to four trunk groups potentially yielding 80 or 800 Mbps of bandwidth, depending on the speed of the interfaces.



Although you can enable trunking for more than eight ports on an FN100 (if more than eight ports exist on your device), the trunking protocol prohibits the use of trunking on more than eight ports at a time. If you enable trunking and establish a valid link for a ninth port, the extra port will be in "hot standby" mode. If connections are broken for any of the original eight trunk ports, the hot standby port will then participate in trunking, provided that it has a valid link to a remote switch which is participating in a trunk group.

You can add ports of different interface speeds to the same trunk groups; however, doing so will cause the higher speed ports to assume the same bandwidth as the lower speed ports, so you effectively lose any transmission speed benefits for the faster port.

To display the Port Trunking window from the FN100 Chassis View:

1. Click to display the **Device** menu.
2. Drag down to **Port Trunking...**, and release. The Port Trunking window, Figure 4-1, will appear.

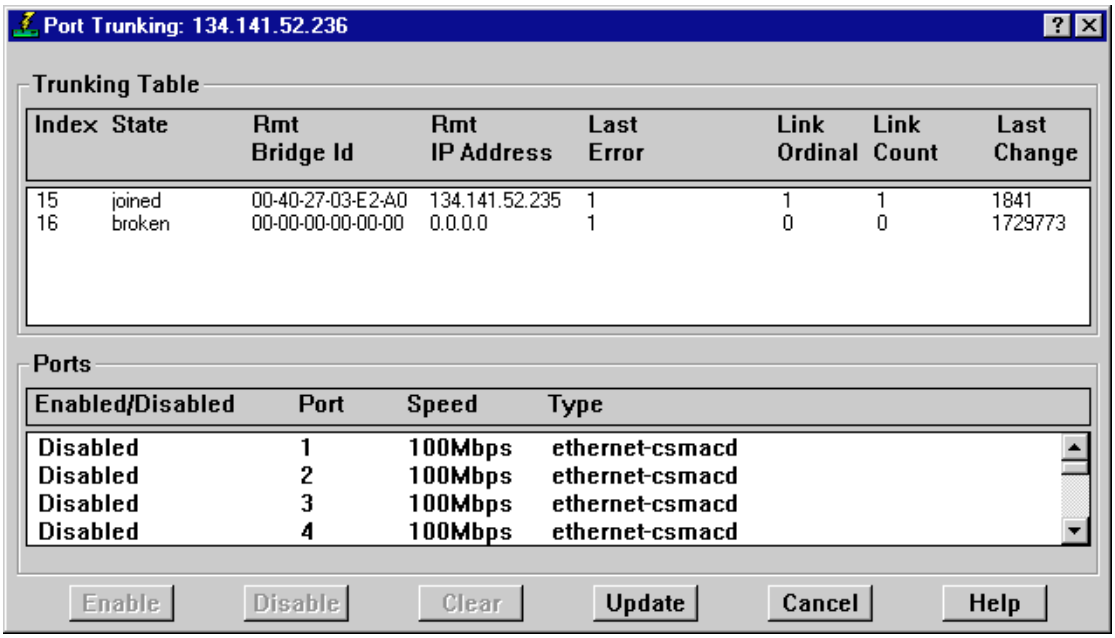


Figure 4-1. The Port Trunking Window

The Port Trunking Window

The Port Trunking window features the trunking table (in the upper portion of the window), which displays the following information about each interface for which trunking is enabled:

Index
Displays the port's sftrunkIfIndex identifier.

State
Indicates the port's trunking condition (sftrunkState). The possible states are:

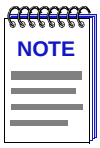
- **closed** — trunking is enabled, and the trunking protocol is attempting to establish a trunk connection, but the port has not yet received any trunking PDUs.
- **oneway** — trunking is enabled, and the trunking protocol is attempting to establish a trunk connection, but incoming trunking PDUs do not indicate that

the FN100's trunking PDUs are being successfully received at the other end of the link.

- **joined** — trunking is enabled, the trunking protocol has established a good trunk connection, and the port is actively participating in the trunk group.
- **perturbed** — trunking is enabled, the trunking protocol has established a good trunk connection, and the port is actively participating in the trunk group; however, the transmission of data packets has been temporarily stopped due to a change in trunk group membership.
- **helddown —** trunking is enabled, but the trunk connection has been rejected. Indicates that an error has been detected and the link is being held out of service until the error condition clears. After a short time-out period, another attempt will be automatically initiated to establish a good trunk connection.
- **broken** — the port has been configured for trunking, but is physically non-operational.

Rmt Bridge Id

Displays the MAC address portion of the remote bridge's bridge ID.



*The **Rmt Bridge Id** field can be used to determine which ports belong to which trunk group. Ports in the same trunk group will have the same remote bridge ID.*

Rmt IP Address

Displays the remote bridge's IP address.

Last Error

Displays a value (1-8) corresponding to a reason for failure when the link is in a **helddown** state. These values and their corresponding reasons for failure include:

- **1** — **none** — no error; the trunking protocol may restart with no error conditions when trunking is activated for a port or when the MIB variable that controls extra trunk groups is modified.
- **2** — **in-bpdu** — a spanning tree BPDU was received, indicating that the connection is not point-to-point, or that the far end of the link does not have trunking enabled.
- **3** — **multiple-bridges** — a different bridge has been connected at the far end of the link, and the trunking protocol will restart.
- **4** — **ack-lost** (acknowledgment lost) — the far end of the link has detected a problem, and the trunking protocol will restart.

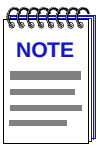
- **5** — **standby** — the trunk group is filled to capacity with other ports; this port is now a hot standby. If another port leaves the trunk group, this port will then be included in the group.
- **6** — **too-many-groups** — the maximum number of groups (4) has been reached, and a new group cannot be added. This port will not be used until the condition clears.
- **7** — **no-ack** (no acknowledgment) — this port has not received a valid trunking packet, and the trunking protocol will restart.
- **8** — **perturbed-threshold** — errors are preventing stabilization, and the trunking protocol will restart.

Link Ordinal
Displays the position of the port's link within its trunk group.

Link Count
Displays the number of links within the port's trunk group.

Last Change
Displays the time (in seconds) since the port's trunk state (sftrunkState) changed.

The lower portion of the Port Trunking window displays the port selection area which, when used in conjunction with the **Enable** and **Disable** buttons at the bottom of the window, allows you to enable or disable trunking for selected ports. The port selection area lists each of the FN100's ports, their trunking state (enabled or disabled), their MIB II ifIndex, ifType, and ifSpeed.



Trunking cannot be enabled for the local management (ppp) port (port 9 or 17, depending on your FN100's port configuration).

The Trunking Table window also features:

Clear
When the **Clear** button is clicked, any selections you have made in the port selection area will be deselected.

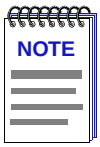
Update
When the **Update** button is clicked, the FN100 will be queried for trunking information, and any changes that have occurred since the window was opened (or since the **Update** button was last clicked) will be reflected in the trunking table.

Enabling and Disabling Trunking

To enable trunking for your FN100 ports using the Port Trunking window:

1. In the port selection list, click on an entry representing a port for which you would like to enable trunking.
2. Click on **Enable**. The trunking table will update to include the new trunking selection.
3. Repeat steps 1 and 2 for each port for which you want to enable trunking.

802.1D Spanning Tree takes about 30 seconds to resolve which FN100 ports in a trunk group are to become forwarding ports. As ports within a trunk group become forwarding ports, traffic within the trunk group will be momentarily halted to guarantee the first-in, first-out ordering of Ethernet packets.



Connections between FN switches must be point-to-point; there cannot be any other devices on those segments. The FN100 ports used for trunking can be in any order. Remember, though, that the switches on both ends of the connections must have trunking enabled for their ports which are used for the connections.

To disable trunking for your FN100 ports using the Port Trunking window:

1. In the port selection list, click on an entry representing a port for which you would like to disable trunking.
2. Click on **Disable**. The trunking table will update to reflect the new trunking selection.
3. Repeat steps 1 and 2 for each port for which you want to disable trunking.

Chapter 5

Workgroup Configuration

Workgroups explained; adding and deleting workgroups from this window

The FN100's Virtual Workgroups window allows you to restrict multicast traffic from being propagated through every bridge port on your device. This optimizes bandwidth by limiting the subnet broadcast traffic to only those ports that require the traffic. You define a virtual work group by specifying a subset of device ports and the type(s) of packets (multicast, unicast, or both) that are to be forwarded by those ports. Each port can belong to more than one work group. In all, you can create up to 100 virtual work groups per switch.

To access the Virtual Workgroups window from the FN100 Chassis View:

1. Click to display the **Device** menu.
2. Drag down to **Workgroups...**, and release. The Virtual Workgroups window, Figure 5-1 will appear.

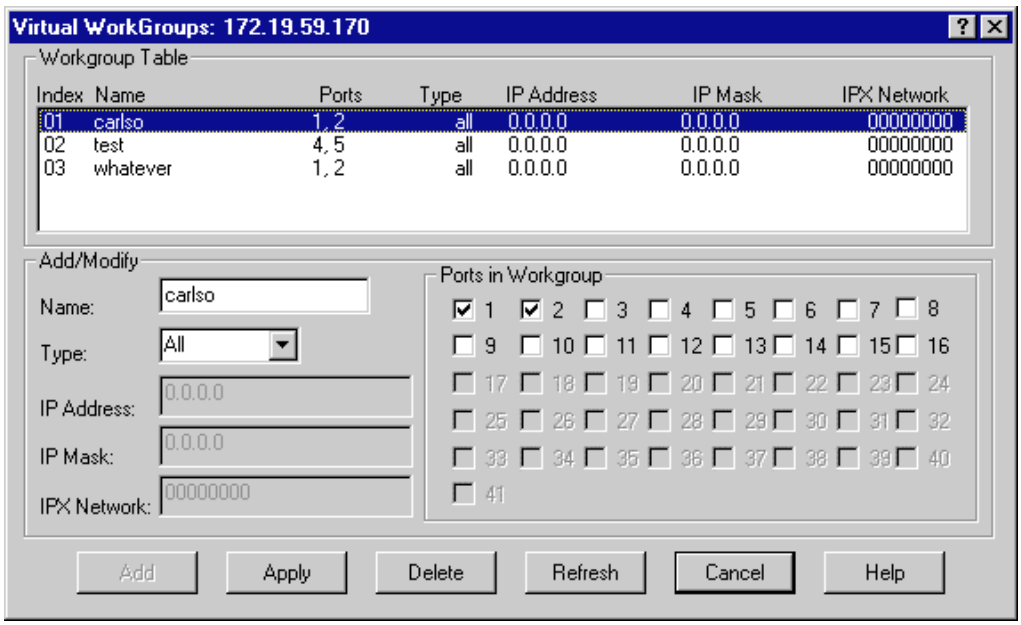


Figure 5-1. Virtual Workgroups Window

You can view and modify existing work groups as well as configure new work groups from this window. The **Workgroup Table** at the top of the window lists each existing work group along with its configuration information. The **Add/Modify** section of this window allows you to set-up the parameters of your work group, including Name and Type. The **Ports in Workgroup** section of the window allows you to choose the ports that will be included in the workgroup.

NOTE

*The **IP Address**, **IP Mask**, and **IPX Network** fields in the **Add/Modify** section of the Virtual Workgroups window are not applicable to the FN100 and are therefore grayed out. Though they may not appear this way upon opening the window, once you select a **Type** of workgroup (see step #3 below), these fields will go gray.*

Configuring a Workgroup

To add or modify a workgroup using the Virtual Workgroups window:

1. To modify an existing workgroup, click on the desired entry in the Workgroup Table. The selected workgroup's configuration information will be reflected in the **Add/Modify** and **Ports in Workgroup** sections of the window.
2. Type a name in the **Name** field in the **Add/Modify** portion of this window. The name can be 1-16 alphanumeric characters. You will use the name to identify the workgroup.

3. Choose the **Type** of workgroup being created or modified. This determines whether ports in this workgroup will forward only multicast packets, only unicast packets, or both multicast and unicast packets. The following are your possibilities:

   - **All** — ports in this workgroup will forward both unicast and multicast packets.
   - **Multicast —** ports in this workgroup will forward only multicast packets.
   - **Unicast —** ports in this workgroup will forward only unicast packets.

4. If necessary, use the **Refresh** button to deselect any ports you have previously selected in the Port Selection area.
5. In the **Ports In Workgroup** area, click on the selection boxes corresponding to the ports you would like to include in this workgroup. Each port is identified by index number. Note that you cannot select the Network Management PPP port for inclusion into a workgroup.
6. Click on **Add** if you are adding a new workgroup, or on **Apply** if you are modifying an existing workgroup. New workgroup entries will be added to the Workgroup Table, and changes to existing workgroups will be reflected in the Workgroup Table.
7. Repeat steps 1-6 to add or modify any additional workgroups.

Deleting a Workgroup

In the Workgroup Table, highlight the work group you would like to delete. Click on **Delete**, the highlighted work group will be deleted. To have this change reflected in the Workgroup Table, click on **Refresh**. The currently defined workgroups will be displayed.

Index