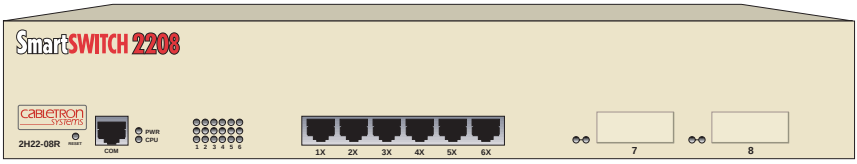
2H22-08R
SmartSwitch 2208
User's Guide



9032385-02

CABLETRON SYSTEMS

Only qualified personnel should perform installation procedures.

NOTICE

Cabletron Systems 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 Cabletron Systems 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 CABLETRON SYSTEMS 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 CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Order Number: 9032385-02 October 1998

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

INDUSTRY CANADA NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CABLETRON SOFTWARE PROGRAM LICENSE

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

   You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

EXCLUSION OF WARRANTY AND DISCLAIMER OF LIABILITY

1. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

   CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

UNITED STATES GOVERNMENT RESTRICTED RIGHTS

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, 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 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

THE FE-100F3 FAST ETHERNET INTERFACE MODULE, FPIM-05 AND FPIM-07 FDDI PORT INTERFACE MODULES, AND APIM-29 ATM PORT INTERFACE MODULE USE CLASS 1 LASER TRANSCEIVERS. READ THE FOLLOWING SAFETY INFORMATION BEFORE INSTALLING OR OPERATING THESE MODULES.

The Class 1 laser transceivers use an optical feedback loop to maintain Class 1 operation limits. This control loop eliminates the need for maintenance checks or adjustments. The output is factory set, and does not allow any user adjustment. Class 1 Laser transceivers comply with the following safety standards:

- 21 CFR 1040.10 and 1040.11 U.S. Department of Health and Human Services (FDA).
- IEC Publication 825 (International Electrotechnical Commission).
- CENELEC EN 60825 (European Committee for Electrotechnical Standardization).

When operating within their performance limitations, laser transceiver output meets the Class 1 accessible emission limit of all three standards. Class 1 levels of laser radiation are not considered hazardous.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or 55 x 10^{-6} watts.

Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm^{-2} or 8 x 10^{3} W m^{2} sr-1.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Cabletron Systems, Inc.**
Manufacturer's Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. J. Solari**
European Representative Address:	**Cabletron Systems Limited** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG13 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 50082-1** **EN 60950**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
Mr. Ronald Fotino	Mr. J. Solari
Full Name	Full Name
Principal Compliance Engineer	Managing Director - E.M.E.A.
Title	Title
Rochester, NH, USA	Newbury, Berkshire, England
Location	Location

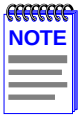
CONTENTS

CHAPTER 1
INTRODUCTION

Welcome to the Cabletron Systems **2H22-08R SmartSwitch 2208 User's Guide**. This guide provides the necessary documentation to install and operate the 2H22-08R SmartSwitch 2208 standalone device and provides information concerning network requirements, installation, troubleshooting, and the use of Local Management.

1.1 USING THIS GUIDE

Read through this guide completely to understand the 2H22-08R device features, capabilities, and Local Management functions. A general working knowledge of Ethernet and IEEE 802.3 type data communications networks and their physical layer components is helpful when using this device.



In this document, the 2H22-08R standalone device is referred to as either the "2H22-08R" or the "standalone."

1.2 STRUCTURE OF THIS GUIDE

This guide is organized as follows:

Chapter 1, **Introduction**, outlines the contents of this manual, and briefly describes the 2H22-08R features. Directions about how to obtain additional help and a list of related manuals are also included.

Chapter 2, **Network Requirements**, explains the network requirements to consider before installing the 2H22-08R.

Chapter 3, **Installation**, provides instructions on how to install the 2H22-08R and connect segments to the device.

Chapter 4, **Troubleshooting**, describes the function of the LANVIEW LEDs, which can help to quickly diagnose network/operational problems.

Chapter 5, **Local Management**, describes how to access Local Management to configure and manage the 2H22-08R.

Appendix A, **Specifications**, contains information on functionality and operating specifications, connector pinouts, environmental requirements, and physical properties.

Appendix B, **FE-100TX, FE-100FX, and FE-100F3 Specifications**, contains information about FE-100TX pinouts and information concerning cable types used with the FE-100FX and FE100-F3.

Appendix C, **Optional Installations and Mode Switch Bank Settings**, describes how to install optional Fast Ethernet Interface Modules and how to set the mode switches.

1.3 2H22-08R OVERVIEW

The 2H22-08R is a Fast Ethernet standalone device that has six RJ45 switched ports and two optional Fast Ethernet Interface Module ports (100BASE-TX, 100BASE-FX, and 100BASE-F3) that provide twisted pair, multimode, and single mode fiber optic cabling connectivity.

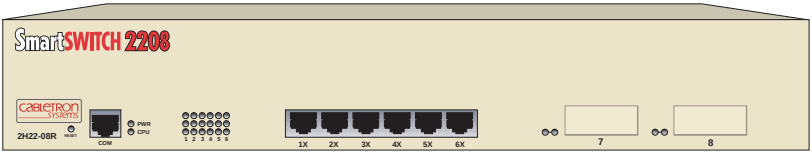


Figure 1-1 The 2H22-08R

The 2H22-08R supports traditional IEEE 802.1d switching (bridging), IEEE 802.Q switching, and Cabletron Systems SECUREFAST Switching Virtual Network technology. The 2H22-08R is used to connect individual high-bandwidth user devices, such as workstations, and provide a central switching point for multiple 10/100 Mbps Fast Ethernet segments.

1.3.1 Auto-Negotiation

Twisted Pair ports on the 2H22-08R can auto-negotiate the type of connection required to provide a link to another device. During Auto-Negotiation, two devices automatically exchange information concerning their operating capabilities. The Auto-Negotiation feature targets the maximum capabilities between the two devices. For example, the 2H22-08R adjusts to 100 Mbps when the device on the other end of the connection can adjust between 10 Mbps or 100 Mbps. If the device on the other end of the connection can only operate at 10 Mbps, then the 2H22-08R adjusts to 10 Mbps operation.

When Auto-Negotiation is supported at both ends of a link, the two devices dynamically adjust to full or half duplex operation based on the maximum capability that can be reached between the two devices. If the device connected to the 2H22-08R cannot auto-negotiate, the 2H22-08R interface operates according to the capabilities of the other device.

1.3.2 Connectivity

The 2H22-08R connects to Ethernet networks or workstations through six RJ45 ports on the front panel. These ports support Category 5 unshielded and shielded twisted pair cables of lengths up to 100 meters. These ports are IEEE 802.3u 100BASE-TX compliant.

The 2H22-08R has two front panel slots (ports 7 and 8) for optional Fast Ethernet Interface Modules (FE-100TX, FE-100FX, and FE-100F3) to support an uplink to 100 Mbps Fast Ethernet backbones or a high speed connection to a local server using twisted pair, multimode or single mode fiber optic cabling.

1.3.3 Runtime IP Address Discovery

This feature enables the 2H22-08R to automatically accept an IP address from a Boot Strap Protocol (BootP) server on the network into NVRAM without requiring a user to enter an IP address through Local Management.

When the 2H22-08R is connected to the network and powered up, Runtime IP Address Discovery (RAD) checks the 2H22-08R for an IP address. If one has not yet been assigned (2H22-08R IP address set to 0.0.0.0), RAD checks to see if any of the 2H22-08R interfaces have a link. If so, RAD sends out Reverse Address Resolution Protocol (RARP) and BootP requests to obtain an IP address from a BootP server on the network.

The RAD requests start out at an interval of 1 second. The interval then doubles after every transmission until an interval of 300 seconds is reached. At this point, the interval remains at 300 seconds. The RAD requests continue until an IP address is received from a BootP server, or an IP address is entered using Local Management.

1.3.4 Remote Monitoring (RMON)

The 2H22-08R supports all Ethernet RMON groups, which include Statistics, Alarms, Events and History as the default groups enabled on all ports, and Capture, Filter, and Host as the groups that are off by default. Cabletron Systems RMON Actions is a vendor-specific extension of RMON and provides the ability to set an "Action" on any SNMP MIB variable. The Action can be triggered by any RMON Event and/or Alarm. The Action can be, for example, to turn a MIB-2 interface off if a broadcast threshold is crossed.

1.3.5 Switching Options

The 2H22-08R provides traditional Switching (802.1D), IEEE 802.1Q, or SECUREFAST Switching Virtual Network Services between all of the front panel interfaces including Fast Ethernet Interface Modules. SECUREFAST Switching and IEEE 802.1Q allows for migration to Virtual Network technologies without requiring the replacement of existing equipment.

1.3.6 Standards Compatibility

The 2H22-08R provides IEEE 802.1, 802.1u, 802.1D and DEC Spanning Tree Algorithm (STA) support to enhance the overall reliability of the network and protect against "loop" conditions. The 2H22-08R supports a wide variety of industry standard MIBs including RFC 1213 (MIB II), RFC 1757 (RMON), RFC 1493 (Bridge MIB), and RFC 1354 (FIB MIB). A full suite of Cabletron Systems Enterprise MIBs provides a wide array of statistical information to enhance troubleshooting.

1.3.7 Year 2000 Compliant

The 2H22-08R has an internal clock that can maintain the current time and date beyond the year 1999.

1.3.8 LANVIEW Diagnostic LEDs

The various conditions of the LANVIEW diagnostic LEDs serve as important troubleshooting aids. They provide an easy way to observe the transmit and receive status of individual ports and overall network operations such as system status, switching configuration, and Fast Ethernet channel usage. **Chapter 4** provides details about the 2H22-08R LANVIEW LEDs.

1.4 LOCAL MANAGEMENT

Management of the 2H22-08R is accomplished using Local Management tools or remote Simple Network Management Protocol (SNMP) management stations. Out-of-band Local Management is accessible through the RS232 COM port on the front panel using a VT100 terminal, or a remote VT100 terminal emulator via a modem connection, and in-band via a Telnet connection. In-band remote management is possible through any SNMP compliant Network Management Software.

Local Management provides the tools to manage the 2H22-08R, and its two Fast Ethernet Interface Modules. It also allows the following tasks to be performed:

- Assign an IP address and subnet mask to the 2H22-08R.
- Select a default gateway and default interface.
- Control local and remote access.
- Designate workstations to receive SNMP traps from the 2H22-08R.

Chapter 5 provides detailed information about Local Management of the 2H22-08R, and its two optional Fast Ethernet Interface Modules. Local Management also provides the features detailed in Section 1.4.1 through Section 1.4.4.

1.4.1 Broadcast Suppression

Broadcast Suppression allows a user to set a desired limit of receive broadcast frames per port/per second to be forwarded out of the other ports on the module up to the set limit. Any broadcast frames above this specified limit are dropped. In the event that broadcast frames are being suppressed, multicast and unicast frames continue to be switched without suppression.

1.4.2 Port Redirect Function

The port redirect function, also referred to as “Port Mirroring,” is a troubleshooting tool used to map traffic from a single source port or multiple source ports to Destination ports(s) within the chassis. This feature functions at the bit level, which allows all packets, including, if desired, those with errors, to be copied and sent to an analyzer or RMON probe that appears as if it is directly connected to the LAN segment of the source port(s).

1.4.3 Full Duplex Switched Ethernet (FDSE)

Each switched Fast Ethernet port on the 2H22-08R supports 10/100 Mbps operation and can be configured to operate in Full Duplex Switched Ethernet (FDSE) mode. FDSE allows each Fast Ethernet port to provide up to 200 Mbps of aggregate throughput bandwidth.

1.4.4 SmartTrunk

SmartTrunk, also referred to as SmartTrunking, is Cabletron Systems’ terminology for load balancing or load sharing. SmartTrunk technology provides an easy-to-implement mechanism to group, or aggregate, multiple physical links together to scale the backbone bandwidth beyond the limitations of a single link. All links are user-configurable so administrators can scale the backbone bandwidth by adding SmartTrunk links. The SmartTrunk benefits are as follows:

- All purchased bandwidth is used.
- Distributed, resilient links increase reliability and performance.
- Multiple technologies are supported within a single trunk for maximum flexibility.

SmartTrunking on the 2H22-08R is available to group the optional Fast Ethernet Interface Module ports 7 and 8.

For more information about SmartTrunk, refer to the Cabletron Systems *SmartTrunk User’s Guide*.

1.5 OPTIONAL FEATURES

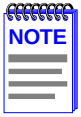
The optional Fast Ethernet Interface Modules provide fiber optic or twisted pair connectivity for uplinks to 100 Mbps Ethernet backbones or high-speed connections to local servers. The Fast Ethernet Interface Modules are listed in Table 1-1.

Table 1-1 Fast Ethernet Interface Modules

P/N	Description	Application
FE-100TX	Uses RJ45 connector	Supports Category 5 Unshielded Twisted Pair (UTP) cabling, which has an impedance of 85 to 111 ohms.
FE-100FX	Uses SC connector	Supports multimode fiber optic cabling.
FE-100F3	Uses SC connector	Supports single mode fiber optic cabling.

1.6 DOCUMENT CONVENTIONS

The following conventions are used throughout this document:



Note symbol. Calls the reader's attention to any item of information that may be of special importance.

Tip symbol. Conveys helpful hints concerning procedures or actions.

Caution symbol. Contains information essential to avoid damage to the equipment.

Warning symbol. Warns against an action that could result in personal injury or death.

Electrical Hazard Warning symbol. Warns against an action that could result in personal injury or death due to an electrical hazard.

In Local Management sections, **Bold type** indicates fields, field values, and commands that can be highlighted or selected by the user.

In Local Management sections, keystrokes are shown in UPPERCASE.

Italic type denotes complete book titles.

1.7 GETTING HELP

For additional support related to this device or document, contact the Cabletron Systems Global Call Center:

World Wide Web	http://www.cabletron.com/
Phone	(603) 332-9400
Internet mail	support@cabletron.com
FTP Login Password	ftp://ftp.cabletron.com/ *anonymous* *your email address*
To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: **TechWriting@cabletron.com** *Make sure to include the document Part Number in the email message.*	

Before calling the Cabletron Systems Global Call Center, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

1.8 RELATED MANUALS

The following manuals may help the user to set up and manage the 2H22-08R:

Cabletron Systems *HSIM-A6DP User's Guide*

Cabletron Systems *HSIM-F6 User's Guide*

Cabletron Systems *HSIM-FE6 User's Guide*

Cabletron Systems *HSIM-W6 Installation Guide*

Cabletron Systems *HSIM-W84 Installation Guide*

Cabletron Systems *HSIM-W87 User's Guide*

Cabletron Systems *HSIM-G01/G09 User's Guide*

Cabletron Systems *Ethernet Technology Guide*

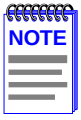
Cabletron Systems *Cabling Guide*

Cabletron Systems *Port Based VLAN User's Guide*

Cabletron Systems *SmartTrunk User's Guide*

These manuals can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://www.cabletron.com/



All documentation for the Cabletron Systems SecureFast VLAN Manager software is contained on the VLAN Manager CD-ROM. The documentation for the HSIM-W6 and HSIM-W84 is on the QuickSET CD-ROM.

CHAPTER 2
NETWORK REQUIREMENTS

Before installing the 2H22-08R or Fast Ethernet Interface Module(s) (FE-100TX, FE-100FX, or FE-100F3) in your network, review the requirements and specifications referred to in this chapter to ensure satisfactory equipment performance. Failure to follow these guidelines may produce poor network performance.

The Cabletron Systems Cabling Guide and SmartTrunk User's Guide, referred to in the following sections, are found on the Cabletron Systems World Wide Web site:
http://www.cabletron.com/

2.1 SmartTrunk

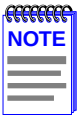
To connect the 2H22-08R to a network so it can take advantage of the SmartTrunk feature, there are certain rules concerning port connections and configurations that must be followed for proper operation. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

2.2 10BASE-T NETWORK

When connecting a 10BASE-T segment to any of the 2H22-08R ports (Interfaces 1 through 8), ensure that the network meets the Ethernet network requirements of the IEEE 802.3 standard for 10BASE-T. Refer to the Cabletron Systems *Cabling Guide* for details.

2.3 100BASE-TX NETWORK

The 2H22-08R, with an FE-100TX installed in ports 7 and 8, provides an RJ45 connection that supports UTP cabling with an impedance between 85 and 111 ohms. The device at the other end of the twisted pair segment must meet IEEE 802.3u 100BASE-TX Fast Ethernet network requirements for the devices to operate at 100 Mbps. Refer to the Cabletron Systems *Cabling Guide* for details.



The 2H22-08R with an FE-100TX installed is capable of operating at either 10 or 100 Mbps. The FE-100TX can automatically sense the speed of the other device and adjusts its speed accordingly.

2.4 100BASE-FX FIBER OPTIC NETWORK

Ports 7 and 8 of the 2H22-08R support the Cabletron Systems FE-100FX and FE-100F3 fiber optic interface modules. The device at the other end of the fiber optic segment must meet the 100BASE-FX Fast Ethernet network requirements to operate at 100 Mbps. Refer to the Cabletron Systems *Cabling Guide* for details.

Multimode Fiber Optic Cable Length

The maximum multimode fiber optic cable length of a 100BASE-FX segment is covered in the Cabletron Systems *Cabling Guide*.

Single Mode Fiber Cable Lengths

The maximum single mode fiber optic length of a 100BASE-FX segment may be no more than 5 km between Data Terminal Equipment (DTE to DTE) in half duplex mode or 20 km (DTE to DTE) in full duplex mode.

Single Mode Cable Loss

Test the single mode fiber optic cable with a fiber optic attenuation test set adjusted for a 1300 nm wavelength. This test verifies that the signal loss is within an acceptable level. The maximum loss for a single mode cable is 10.0 dB.

CHAPTER 3
INSTALLATION

Only qualified personnel should install the 2H22-08R.

This chapter provides the instructions required to install the 2H22-08R. Follow the order of the sections listed below to correctly install the 2H22-08R.

- Required Tools (Section 3.1)
- Unpacking the 2H22-08R (Section 3.2)
- Installing Options (Section 3.3)
- Installing the 2H22-08R (on a shelf or tabletop, or into a standard rack) (Section 3.4)
- Connecting to the Network (Section 3.6)
- Completing the Installation (Section 3.7)

3.1 REQUIRED TOOLS

A Phillips screwdriver is required to install the 2H22-08R in a rack.

3.2 UNPACKING THE 2H22-08R

To unpack the 2H22-08R and verify the contents of the shipment, proceed as follows:

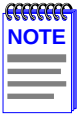
1. Open the carton and remove the packing material protecting the 2H22-08R.
2. Verify the contents of the carton as listed in Table 3-1.

Table 3-1 Contents of 2H22-08R Carton

Item	Quantity
2H22-08R	1
Antistatic Wrist Strap	1
Console Cable Kit	1
Rackmount Kit	1
Strain-Relief Bracket	1
Power Cord	2

3. Remove the black and yellow tape seal on the non-conductive bag to remove the 2H22-08R.
4. Perform a visual inspection of the device for any signs of physical damage. If there are any items missing or damaged, contact Cabletron Systems Global Call Center as described in Section 1.7.

3.3 INSTALLING OPTIONS



Install any optional equipment before proceeding to Section 3.4.

If the 2H22-08R is to be installed with an optional Fast Ethernet Interface Module, refer to Appendix C for installation instructions.

3.4 INSTALLING THE 2H22-08R

The 2H22-08R may be installed on a tabletop, shelf, or in a 19-inch rack. Section 3.4.1 provides the rules and instructions for a tabletop and shelf installations, and Section 3.4.2 provides the rules and instructions for a rackmount installation.

CAUTION

To ensure proper ventilation and prevent overheating, leave a minimum clearance space of 5.1 cm (2.0 in) at the left, right, and rear of the 2H22-08R.

3.4.1 Tabletop and Shelf Installations

Tabletop and shelf installations must be within reach of the network cabling and meet the requirements listed below:

- Locate the 2H22-08R within seven feet of an appropriately grounded power source and an unrestricted surface area as shown in Figure 3-1 that meets the power supply requirements listed in Appendix A.
- In a shelf installation, the shelf must support 13.6 kg (30 lb) of static weight for each 2H22-08R.
- Maintain a temperature of between 5°C (41°F) and 40°C (104°F) at the installation site with fluctuations of less than 10°C (18°F) per hour.

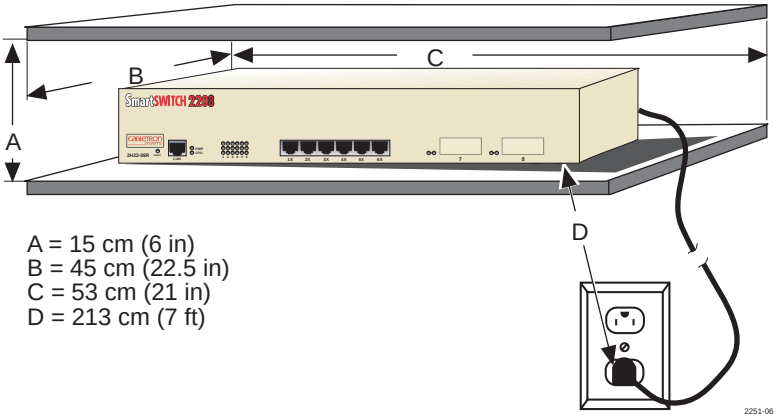


Figure 3-1 Tabletop or Shelf Installation

3.4.2 Rackmount Installation

Rackmount installations must be within reach of the network cabling and meet the requirements listed below:

- Locate the 2H22-08R within seven feet of an appropriately grounded power source and an unrestricted surface area as shown in Figure 3-1 that meets the power supply requirements listed in Appendix A.
- Maintain a temperature of between 5°C (41°F) and 40°C (104°F) at the installation site with fluctuations of less than 10°C (18°F) per hour.

The 2H22-08R is shipped with a strain-relief bracket for cable management. The rackmount kit contains the rackmount brackets and mounting screws for installing it in a 19-inch rack.

Before installing the 2H22-08R into a rack, ensure that the rack supports the device(s) without compromising the stability of the rack. Otherwise, personal injury and/or equipment damage may result.

Attaching the Strain-Relief Bracket

Use of the strain-relief bracket is optional, but recommended to reduce cable damage and maintain an orderly environment. Attach the strain-relief bracket to the front of the 2H22-08R as follows:

1. Locate the strain-relief bracket and four 8-32 x 3/8-inch pan-head screws in the rackmount kit.

Do not attempt to attach the strain-relief bracket with screws other than the 8-32 x 3/8-inch screws included with the 2H22-08R. Use of longer screws may damage the unit.

2. Attach the strain-relief bracket to the bottom of the 2H22-08R using the four 8-32 x 3/8-inch pan-head screws (Figure 3-2).

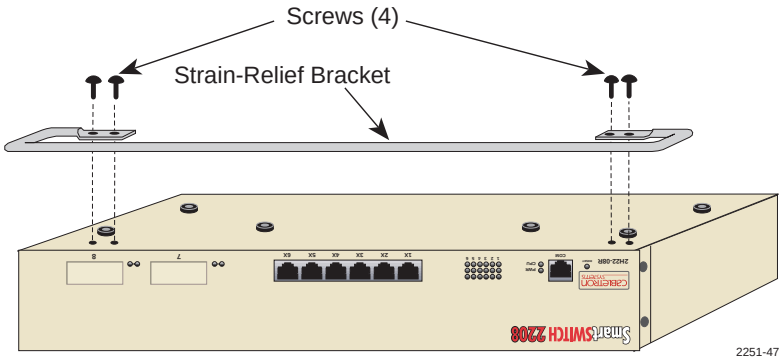


Figure 3-2 Attaching the Strain-Relief Bracket

Rack Mounting the 2H22-08R

Proceed as follows to install the 2H22-08R into a 19-inch rack.

1. Remove and discard the four cover screws (two from each side) located along the front edges of each side of the 2H22-08R.

2. Locate the four 6-32 x 3/8-inch flathead cover replacement screws in the rackmount kit. Use these screws to attach the rackmount brackets to the 2H22-08R as shown in Figure 3-3.

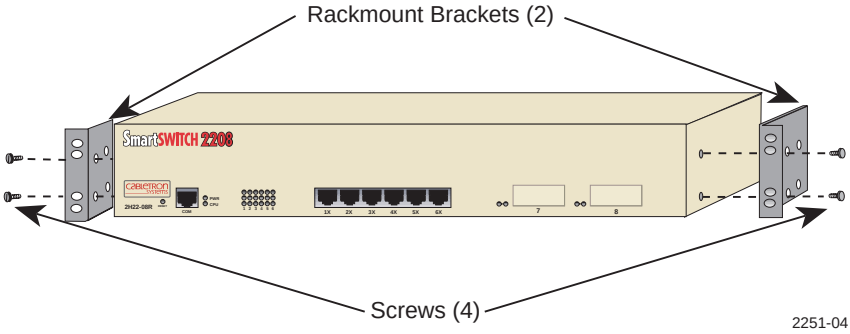


Figure 3-3 Installing the Rackmount Brackets

3. With the mounting brackets installed, position the 2H22-08R between the vertical frame members of the 19-inch rack and fasten it securely with user supplied mounting screws as shown in Figure 3-4.

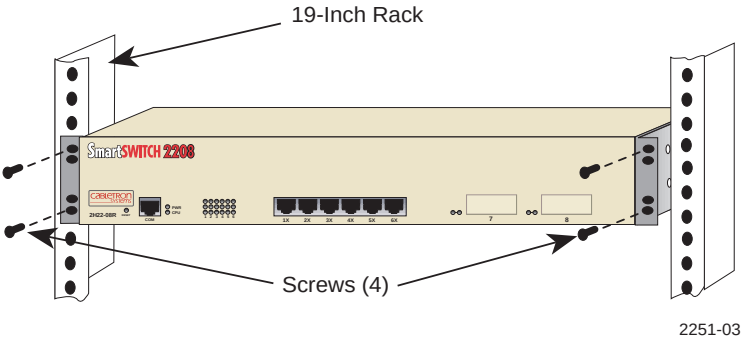


Figure 3-4 Installing the 2H22-08R in a Rack

3.5 CONNECTING POWER TO THE 2H22-08R

NOTE

The 2H22-08R has a primary and redundant power supply. Both power supplies have automatic voltage sensing that allows connection to power sources ranging from 100–125 Vac, 2.0 A or 200–240 Vac, 1.0 A, 50/60 Hz.

To connect the 2H22-08R to the power sources, proceed as follows:

1. Insert the connector of each power cord into the two power supplies and insert the plug of each power cord from the 2H22-08R into a grounded wall outlet, see Figure 3-5. To take advantage of the load sharing and redundancy capabilities, each power cord must be plugged into a dedicated ac outlet. The POWER LED turns on (green) and the CPU LED turns on (green) briefly.

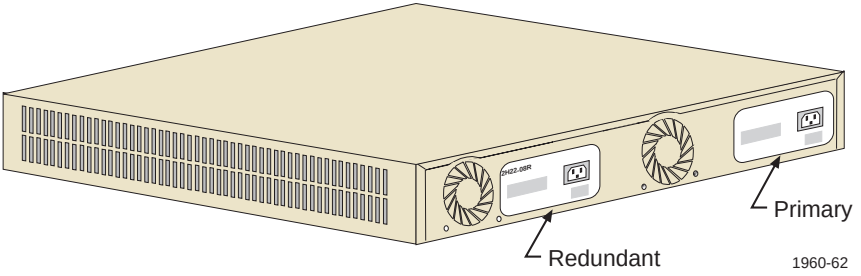
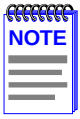


Figure 3-5 2H22-08R Rear View

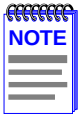


It takes approximately one minute for the 2H22-08R to boot up.

2. Observe the LANVIEW LEDs. After a successful boot, the CPU LED turns on (green). If the PWR LED is not green after one minute and turns amber, there is no power redundancy. Check the power cord connections and the power source. If there are no problems with the power cord connections or power source and the PWR LED is still not green, contact the Cabletron Systems Global Call Center. Refer to Section 1.7 for details.

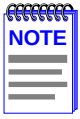
3.6 CONNECTING TO THE NETWORK

This section provides the procedures for connecting twisted pair and fiber optic segments from the network or other devices to the 2H22-08R.



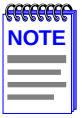
If the 2H22-08R is being installed in a network using SmartTrunking, there are rules concerning the network cable and port configurations that must be followed for SmartTrunking to operate properly. Before connecting the cables, refer to the Cabletron Systems *SmartTrunk User's Guide* for configuration information.

Ports 1 through 6 on the 2H22-08R have RJ45 connectors for twisted pair connections. Ports 7 and 8 support FE-100TX, FE-100FX, or FE-100F3 Fast Ethernet Interface Modules. The FE-100TX has an RJ45 connector for a twisted pair cable connection. The FE-100FX and FE-100F3 have SC connectors for fiber optic cable connections.



Refer to the Cabletron Systems *Cabling Guide* to make a twisted pair connection to an FE-100TX, or a fiber optic cable connection to an FE-100FX or FE-100F3 for port slot 7 or 8.

3.6.1 Connecting a Twisted Pair Segment to the FE-100TX



To ensure proper operation, use only Category 5 Unshielded Twisted Pair (UTP) cabling that has an impedance of 85 to 111 ohms.

An FE-100TX installed in port slot 7 and/or 8 has an internal crossover switch. When connecting a workstation, use a straight-through cable and set the Fast Ethernet Interface Module crossover switch shown in Figure 3-6 to the straight-through position marked with =. To connect networking devices, such as another switch, repeater, or router, use a crossover cable or flip the crossover switch to the crossed over position marked with an X as shown in Figure 3-6.

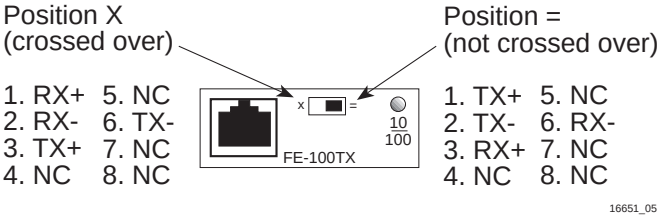


Figure 3-6 FE-100TX Crossover Switch

A schematic of a crossover cable is shown in Figure 3-7. If the wires do not cross over, use the switch on the FE-100TX to internally cross over the RJ45 port.

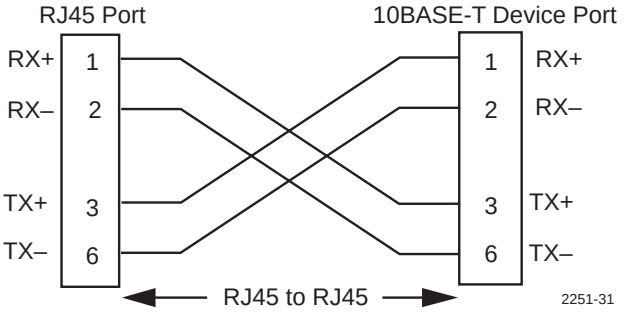


Figure 3-7 Cable Pinouts - RJ45 Crossover Cable

Connect an FE-100TX to a Twisted Pair segment as follows:

1. Ensure that the device connected to the other end of the segment is powered on.
2. Connect the twisted pair segment by inserting the RJ45 connector into the RJ45 port on the module shown in Figure 3-8.

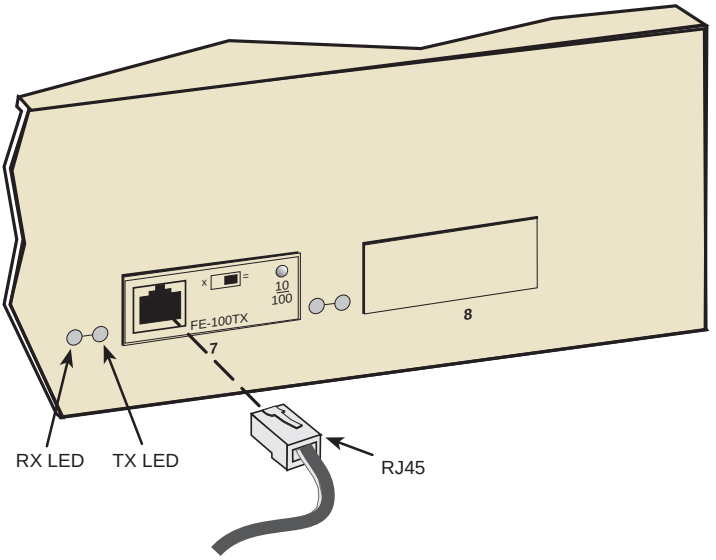


Figure 3-8 FE100-TX Port

3. Verify that a link exists by checking that the port RX LED is on (flashing amber, blinking green, or solid green). If the RX LED is off and the TX LED is not blinking amber, perform the following steps until the RX LED is on:
   a. Verify that the 100BASE-TX device at the other end of the twisted pair segment is powered up.
   b. Verify that the RJ45 connector on the twisted pair segment has the proper pinouts.
   c. Check the cable for continuity.

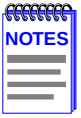
d. Make sure that the twisted pair connection meets the cable specifications outlined in the *Cabletron Systems Cabling Guide*. Refer to Section 1.8, **Related Manuals**.

e. Confirm that the crossover switch is in the correct position.

If a link is not established, refer to Chapter 4, **Troubleshooting**, for details on how to fix the problem.

3.6.2 Connecting a Fiber Optic Segment to the FE-100FX and FE-100F3

The FE-100FX and FE-100F3 have SC style network ports. See Figure 3-9. Cabletron Systems offers optional fiber optic cables that use SC style connectors. The ST connectors are keyed to ensure proper crossover of the transmit and receive fibers.



An odd number of crossovers (preferably one) must be maintained between devices so that the transmit port of one device is connected to the receive port of the other device and vice versa.

If the fiber optic cable being used has SC style connectors that do not resemble MIC style connectors, or has SC connectors on one end and a different type on the other, such as ST connectors, ensure that the proper crossing over occurs.

Fiber Optic Network Connection

1. Remove the protective plastic covers from the fiber optic ports on the applicable port on the module and from the ends of the connectors.

The FE-100F3 uses Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. Before viewing the output optical port, remove power from the network adapter.

CAUTION

Do not touch the ends of the fiber optic strands, and do not let the ends come in contact with dust, dirt, or other contaminants. Contamination of the ends causes problems in data transmissions. If the ends become contaminated, clean them with alcohol using a soft, clean, lint-free cloth.

2. Insert one end of the SC connector into the FE-100FX or FE-100F3 installed in the 2H22-08R. See Figure 3-9.

3. At the other end of the fiber optic cable, attach the SC connector to the other device.

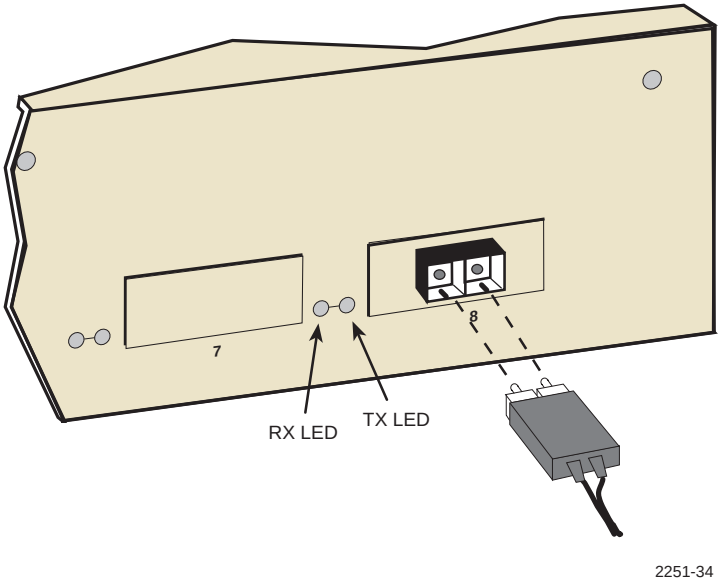


Figure 3-9 FE-100FX and FE-100F3 Ports

4. Verify that a link exists by checking that the port RX LED is on (flashing amber, blinking green, or solid green). Refer to Chapter 4 for further LED indications and descriptions. If the RX LED is off and the TX LED is not blinking amber, perform the following steps until the RX LED is on:

   a. Check that the power is turned on for the device at the other end of the link.

   b. Verify proper crossover of fiber strands between the applicable port on the 2H22-08R and the fiber optic device at the other end of the fiber optic link segment.

   c. Verify that the fiber connection meets the dB loss specifications outlined in Section 2.4.

If a link has not been established, contact the Cabletron Systems Global Call Center. Refer to Section 1.7 for details.

3.7 COMPLETING THE INSTALLATION

After installing the 2H22-08R and any optional Fast Ethernet Interface Modules, and making the connections to the network, proceed as follows:

1. Secure the cables by running the cables along the strain-relief bracket and tying them to the strain-relief bracket using cable ties.

2. The 2H22-08R is now ready to be set up through Local Management. Refer to Chapter 5, **Local Management**, for information on how to access and use Local Management to configure the 2H22-08R.

CHAPTER 4
TROUBLESHOOTING

This chapter provides information concerning the following:

- Using the LANVIEW diagnostic and status monitoring system
- Troubleshooting network and 2H22-08R operational problems
- Using the RESET button

4.1 USING LANVIEW

The 2H22-08R uses Cabletron Systems built-in visual diagnostic and status monitoring system called LANVIEW. The LANVIEW LEDs (Figure 4-1) allow quick observation of the network status to aid in the diagnosing of network problems. Refer to Table 4-1 for a description of the LEDs.

For a functional description of the LANVIEW LED on the optional Fast Ethernet Interface Module (FE-100TX), refer to Section 4.2.

NOTE

The terms **Flashing**, **Blinking**, and **Solid** used in the following table indicate the following:

Flashing indicates an irregular LED pulse.

Blinking indicates a steady LED pulse.

Solid indicates a steady LED light. No pulsing.

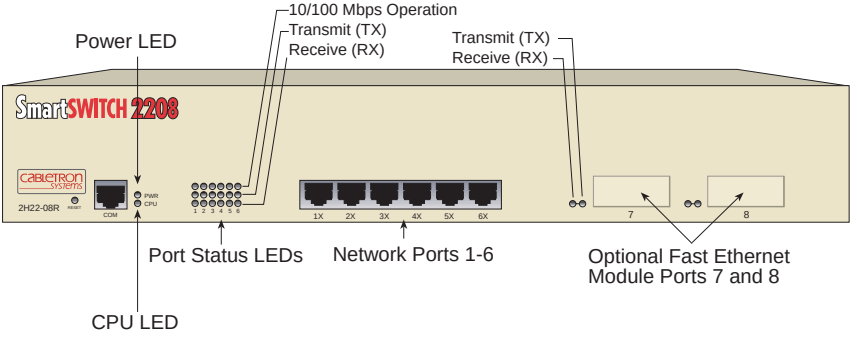


Figure 4-1 2H22-08R SmartSwitch 2208 LANVIEW LEDs

Table 4-1 LANVIEW LEDs

LED	Color	State	Explanation or Recommended Action
CPU	Off	Power off.	Power up chassis.
	Red	**Blinking**. Hardware failure has occurred.	Contact Cabletron Systems Global Call Center (GCC).
		Solid. Resetting, normal power up reset.	No action.
	Amber	**Blinking**. Crippled.	Contact Cabletron Systems Global Call Center.
		Solid. Testing.	No action.
	Green	**Solid**. Functional.	No action.
	Amber and Green	Booting. Blinks amber and green while booting.	No action.
RX	Off	No link. No activity or port in standby. Port enabled or disabled.	No error.
	Green	**Solid**. Port enabled, link, no activity.	No error.
		Blinking. Port disabled, link.	No error.
	Amber	**Flashing**. Port enabled, link, activity.	No error.
	Red	Diagnostic failure.	Contact Cabletron Systems GCC for assistance.
TX	Off	Port enabled, and no activity.	Should flash green every 2 seconds indicating BPDUs being sent if STA is enabled and there is a valid link.
	Green	**Flashing**. Indicates activity. Rate indicates data rate.	No action.
	Amber	**Blinking**. Port in standby, link.	Port may be disabled due to Spanning Tree.
	Red	**Flashing**. Indicates collision rate.	No action.
		Solid. Diagnostic failure.	Contact Cabletron Systems GCC for assistance.

Table 4-2 Port 1-6 10/100 LED Indications

LED	Color	Explanation
10/100	Off	No link or no cable attached. There is a link and the port is operating at 10 Mbps operation.
	Green	Link. Port is operating at 100 Mbps.

4.2 FE-100TX LED

The optional FE-100TX for the 2H22-08R has one LED labeled 10/100. The 10/100 LED together with the receive LED allows the user to determine the Link status and the operating speed of the Fast Ethernet Interface Module. The 10/100 LED and the Receive (RX) LED are shown in Figure 4-2. Table 4-2 and Table 4-3 provide a functional description of the FE-100TX LED when the RX LED is on or off, respectively.

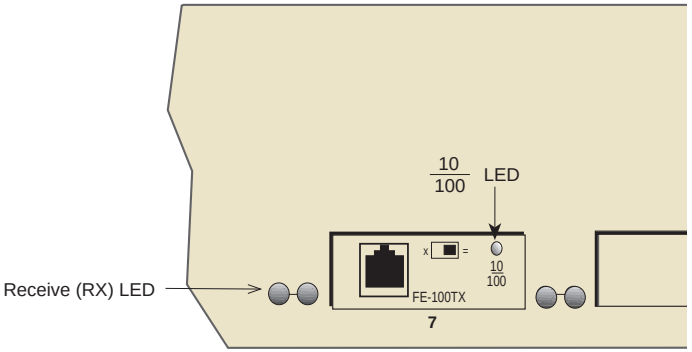


Figure 4-2 FE-100TX LED

NOTE

A link exists if the associated port (port 7or 8) Receive (RX) LED is on. No Link exists if the associated port (port 7 or 8) Receive (RX) LED is off.

Table 4-3 FE-100TX LED Indications

LED	Color	Description
10/100	Off	No link or no cable attached. FE-100TX is forced or Auto-Negotiates to 10 Mbps operation.
	Green	FE-100TX is operating at 100 Mbps.

4.3 TROUBLESHOOTING CHECKLIST

If the 2H22-08R is not working properly, refer to Table 4-4 for a checklist of possible problems, causes, and recommended actions to resolve the problem.

Table 4-4 Troubleshooting Checklist

Problem	Possible Cause	Recommended Action
All LEDs are OFF.	Loss of Power to the 6C105 chassis.	Check the proper connection of the power cable and its access to a live outlet.
	2H22-08R not properly installed.	Check the installation.
No Local Management Password screen.	Autobaud enabled.	Press ENTER (RETURN) (may take up to four times).
	Terminal setup is not correct.	Refer to Chapter 5 for proper setup procedures.
	Improper console cable pinouts.	Refer to Appendix A for proper console port pinouts.
Cannot contact the 2H22-08R from in-band management.	Improper Community Names Table.	Refer to Chapter 5 for Community Names Table setup.
	2H22-08R does not have an IP address.	Refer to Chapter 5 for IP address assignment procedure.
	Port is disabled.	Enable port.
	No link to device.	Check link to device.

Table 4-4 Troubleshooting Checklist (Continued)

Problem	Possible Cause	Recommended Action
Port(s) goes into standby for no apparent reason.	2H22-08R detects a looped condition.	Review network design and delete unnecessary loops.
User parameters (IP address, Device and Module name, etc.) are lost when the 2H22-08R is powered down or the front panel RESET button is pressed.	Mode switch (7), NVRAM Reset, was changed sometime before either cycling power or pressing the RESET button, causing the user-entered parameters to reset to factory default settings. Clear NVRAM was set through Local Management.	Reenter the lost parameters as necessary. Call Cabletron Systems Global Call Center if problem continues.

4.4 USING THE RESET BUTTON

The RESET button, located to the left of the COM port on the 2H22-08R, (refer to Figure 4-3) resets the 2H22-08R processor without affecting the NVRAM.

NOTE

The RESET button may be used in conjunction with Mode Switch 7 (Clear NVRAM), described in Appendix C, to clear user-entered parameters such as IP addresses and Community Names and to replace them with the 2H22-08R default settings. It is only necessary to use this method of clearing NVRAM when it is not possible to access Local Management.

Clearing NVRAM may also be performed via Local Management. Section 5.7.11, Clearing NVRAM, describes how to perform this procedure.

CAUTION

Pressing the RESET button resets the device, and all current switching being performed by the device is halted. A network downtime of up to two minutes will result from this action.

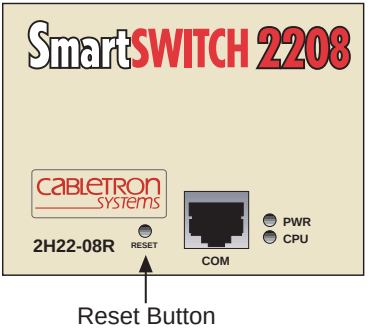


Figure 4-3 RESET Button

To reset the 2H22-08R processor, press and release the RESET button. The device processor goes through a reset process of approximately 20 seconds. Additional downtime may be added as the 2H22-08R reenters the network.

CHAPTER 5
LOCAL MANAGEMENT

This chapter explains how to set up a management terminal to the 2H22-08R, and access the 2H22-08R using its Local Management screens and commands.

5.1 OVERVIEW

Local Management is a series of management screens that allows you to configure the 2H22-08R. The management screens allow you to do the following tasks:

- Assign IP addresses and subnet masks to the 2H22-08R
- Assign a default gateway
- Control access to the 2H22-08R by establishing Community Names
- Download a new image of operating software
- Designate which Network Management Workstations receive SNMP traps from the 2H22-08R
- View switch, interface, and RMON statistics
- Assign ports to operate in Auto-Negotiate, standard or full duplex mode
- Perform load sharing by SmartTrunking ports
- Configure optional Fast Ethernet Interface Modules of the 2H22-08R
- Clear NVRAM, allows user-entered parameters such as an IP address or Community Names to be deleted.

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port of the 2H22-08R
- Remotely using a VT type terminal connected through a modem
- In-band through a Telnet connection

5.2 LOCAL MANAGEMENT KEYBOARD CONVENTIONS

All key names display as capital letters in this manual. Table 5-1 explains the keyboard conventions and the key functions that are used.

Table 5-1 Keyboard Conventions

Key	Function
ENTER Key RETURN Key	These are selection keys that perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESCAPE (ESC) Key	This key enables an escape from a Local Management screen without saving changes. For example, “Press ESC twice” means the ESC key must be pressed quickly two times.
SPACE bar BACKSPACE Key	These keys cycle through selections in some Local Management fields. Use the SPACE bar to cycle forward through selections and use BACKSPACE to cycle backward through selections.
Arrow Keys	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
[–] Key	This key decreases values from a Local Management increment field. For example, “Press [–]” means to press the minus sign key.
DEL Key	The DEL (Delete) key removes characters from a Local Management field. For example, “Press DEL” means to press the Delete key.

5.3 MANAGEMENT TERMINAL SETUP

Use one of the following systems to access Local Management:

- An IBM or compatible PC running a VT series emulation software package
- A Digital Equipment Corporation VT100 type terminal
- A VT type terminal running emulation programs for the Digital Equipment Corporation VT100 series
- A remote VT100 type terminal via a modem connection
- In-Band via a Telnet connection

5.3.1 Console Cable Connection

Use the Console Cable Kit provided with the 2H22-08R to attach the management terminal to the 2H22-08R COM port as shown in Figure 5-1.

Connect an IBM VT terminal device, running the VT terminal emulation, to the 2H22-08R as follows:

1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the 2H22-08R.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 adapter (supplied in the kit).
3. Connect the RJ45-to-DB9 adapter to the communications port on the PC.

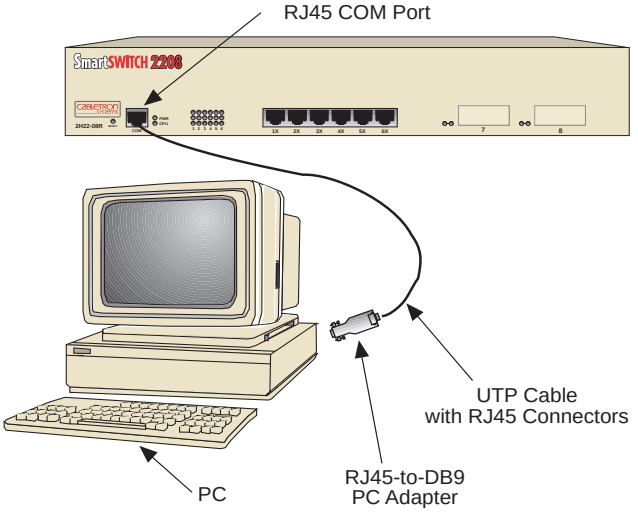


Figure 5-1 Management Terminal Connection (PC Connection)

5.3.2 Uninterruptible Power Supply Monitoring

If the 2H22-08R is connected to an American Power Conversion Uninterruptible Power Supply (UPS) device for protection against the loss of power, a connection from the 2H22-08R COM port to the UPS can be made to monitor the power status of the UPS. To use the COM port for this purpose, it must be reconfigured to support the UPS connection using the procedure described in Section 5.7.10. Refer to the UPS documentation for details on how to access the status information.

Use the Console Cable Kit provided with the 2H22-08R to attach the UPS to the 2H22-08R COM port as shown in Figure 5-2.

To connect the UPS device to the COM port of the 2H22-08R, proceed as follows:

1. Connect the RJ45 connector at one end of the cable to the COM port on the 2H22-08R.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 male (UPS) adapter, Cabletron Systems Part No. 9372066.
3. Connect the RJ45-to-DB9 male (UPS) adapter to the female DB9 port on the rear of the UPS device (refer to the particular UPS device's user instructions for more specific information about the monitoring connection).

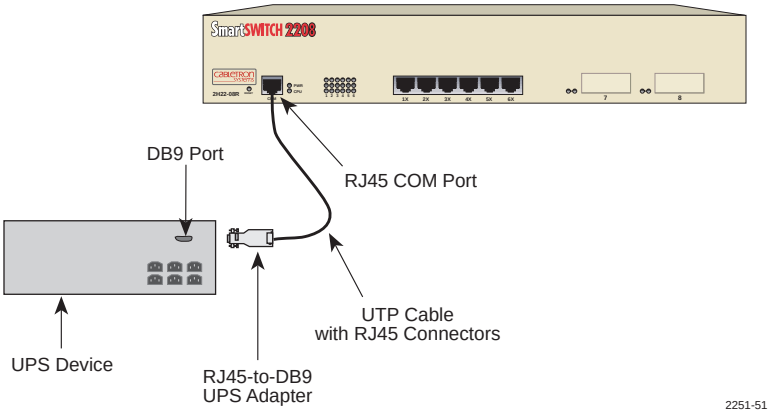


Figure 5-2 Uninterruptible Power Supply (UPS) Connection

5.3.3 Management Terminal Setup Parameters

Table 5-2 lists the setup parameters for the local management terminal.

Table 5-2 VT Terminal Setup

Display Setup Menu	
Columns ->	80 Columns
Controls ->	Interpret Controls
Auto Wrap ->	No Auto Wrap
Scroll ->	Jump Scroll
Text Cursor ->	Cursor
Cursor Style ->	Underline Cursor Style
General Setup Menu	
Mode ->	VT100, 7 Bit Controls
ID number ->	VT100ID
Cursor Keys ->	Normal Cursor Keys
Power Supply ->	UPSS DEC Supplemental
Communications Setup Menu	
Transmit ->	2400, 4800, 9600, 19200
Receive ->	Receive=Transmit
XOFF ->	XOFF at 64
Bits ->	8 bits
Parity ->	No Parity
Stop Bit ->	1 Stop Bit
Local Echo ->	No Local Echo
Port ->	DEC-423, Data Leads Only
Transmit ->	Limited Transmit
Auto Answerback ->	No Auto Answerback
Keyboard Setup Menu	
Keys ->	Typewriter Keys
Auto Repeat ->	any option
Keyclick ->	any option
Margin Bell ->	Margin Bell
Warning Bell ->	Warning Bell

5.3.4 Telnet Connections

Once the 2H22-08R has a valid IP address, you can establish a Telnet session with Local Management from any TCP/IP based node on the network. Telnet connections to the 2H22-08R require the Community Name passwords assigned at the SNMP Community Names screen of the 2H22-08R.

For information about setting the IP address, refer to Section 5.7.

For information about assigning Community Names, refer to Section 5.8.

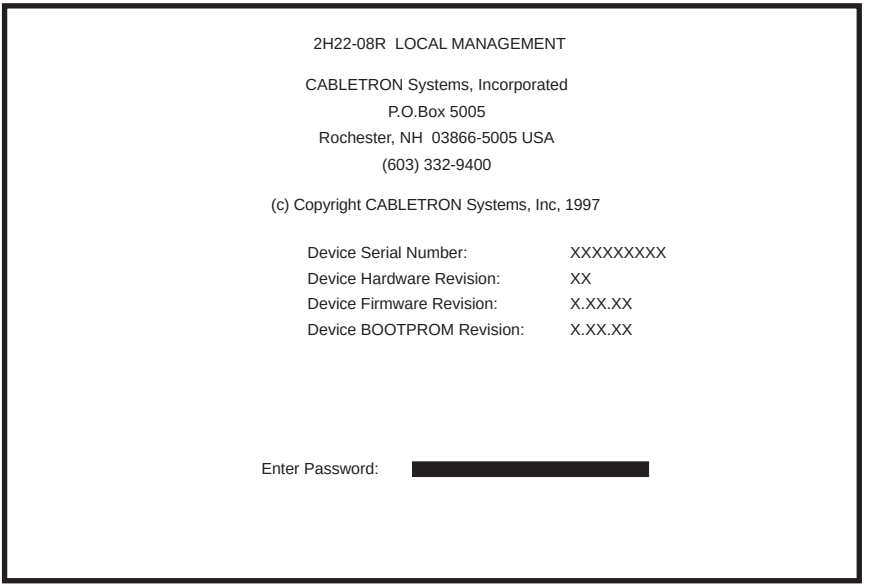
Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

5.4 ACCESSING LOCAL MANAGEMENT

Access to Local Management is controlled through the Local Management Password screen shown in Figure 5-3. Whenever a connection is made to the 2H22-08R, the Password screen displays. Before continuing, you must enter a password (community name) which is compared to the previously stored passwords. The level of access allowed to a user depends on the password. To set or change passwords refer to Section 5.8.1.

The following steps describe the procedure to access Local Management:

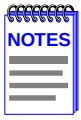
1. Turn on the terminal. Press ENTER (this may take up to four times, because the COM port of the 2H22-08R auto-senses the baud rate of the terminal) until the Local Management Password screen displays.



22511-12

Figure 5-3 Local Management Password Screen

2. Enter the password and press ENTER. The default super-user access password is "*public*" or press ENTER.



A user's password is one of the Community Names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access accorded that Community Name. Refer to Section 5.8.

If an invalid password is entered, the terminal beeps and the cursor returns to the beginning of the password entry field.

When entering a valid password, the associated access level displays at the bottom of the screen and the Main Menu screen displays.

If no activity occurs for several minutes, the Password screen reappears and the session ends.

5.4.1 Navigating Local Management Screens

The 2H22-08R Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens.

The 2H22-08R support three modes of switch operation. The switching modes are as follows:

- 802.1d Switching (traditional switching)
- 802.1Q Switching (802.1Q port based switching)
- SECURE FAST VLAN (Cabletron Systems SecureFast switching)

Depending on the Operational Mode set for the device, the hierarchy of Local Management screens differs as shown in Figure 5-4, Figure 5-5 and Figure 5-6. Refer to the appropriate figure that relates to the Operational Mode set for the device to see the applicable Local Management screen hierarchy.

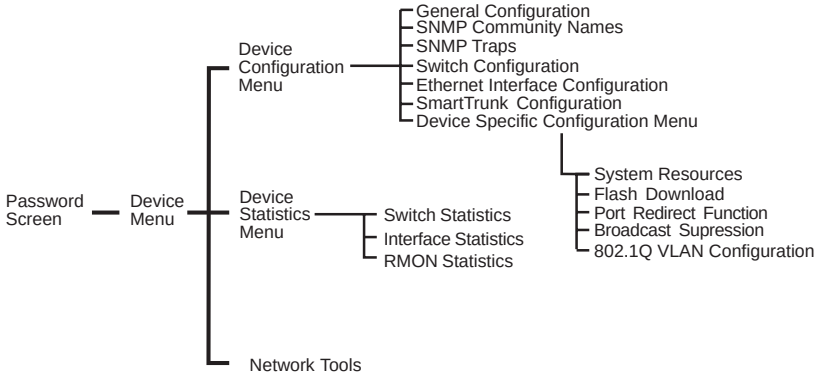


Figure 5-4 802.1d Switching Mode, LM Screen Hierarchy

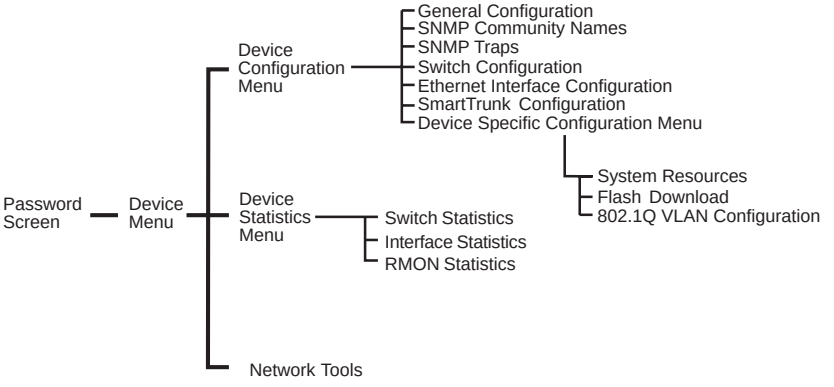


Figure 5-5 802.1Q Switching Mode, LM Screen Hierarchy

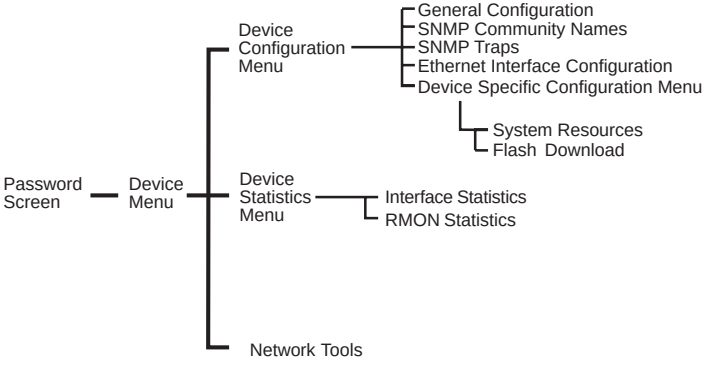


Figure 5-6 SecureFast VLAN Mode, LM Screen Hierarchy

5.4.2 Selecting Local Management Menu Screen Items

Select items on a menu screen by performing the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press ENTER. The selected menu item displays on the screen.

5.4.3 Exiting Local Management Screens

There are two ways to exit the Local Management (LM) screens.

Using the Exit Command

To exit LM using the EXIT screen command, proceed as follows:

1. Use the arrow keys to highlight the **EXIT** command at the bottom of the Local Management screen.
2. Press ENTER. The Local Management Password screen displays and the session ends.

Using the RETURN Command

To exit LM using the RETURN command, proceed as follows:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.

The user can also exit Local Management screens by pressing ESC twice. This exit method does not warn about unsaved changes and all unsaved changes are lost.

3. Exit from Local Management by repeating steps 1 and 2 until the Device Menu screen displays.
4. To end the LM session, use the arrow keys to highlight the **RETURN** command at the bottom of the Device Menu screen.
5. Press ENTER. The Local Management Password screen displays and the session ends.

5.5 DEVICE MENU SCREEN

The Device Menu screen, shown in Figure 5-7, is the access point for all Local Management screens.

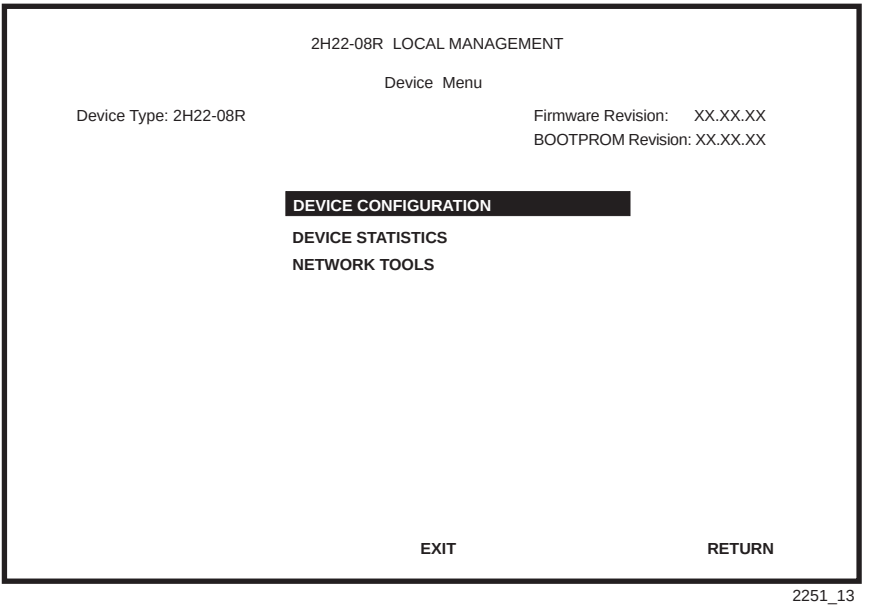


Figure 5-7 Device Menu Screen

The following explains each of the Device Menu menu items shown in Figure 5-7:

DEVICE CONFIGURATION

The Device Configuration screen provides access to the Local Management screens that are used to configure the 2H22-08R and the Device Specific Configuration Menu screen. The Device Specific Configuration Menu screen provides access to the screens that allows you to check the 2H22-08R resources and set operating parameters specific to each port.

For details about the Device Configuration Menu screen, refer to Section 5.6. For details about the Device Specific Configuration Menu screen, refer to Section 5.12.

DEVICE STATISTICS

The Device Statistics screen provides statistics and performance information for the 2H22-08R. For details, refer to Section 5.17.

NETWORK TOOLS

The Network Tools function resides on the 2H22-08R and consists of a series of commands that allow you to access and manage network devices. Section 5.21 explains using the Network Tools utility.

5.6 DEVICE CONFIGURATION MENU SCREEN

NOTE

The SWITCH CONFIGURATION and SMARTTRUNK CONFIGURATION menu items on the Device Configuration Menu screen will not display if the operational mode of the device has been set to SECURE FAST VLAN:

Section 5.7.9 provides instructions for setting the operational mode.

The Device Configuration Menu screen, Figure 5-8, provides access to Local Management screens. These screens allow you to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, configure switch parameters and configure 2H22-08R ports.

To access the Device Configuration Menu screen from the Device Menu screen, use the arrow keys to highlight the **DEVICE CONFIGURATION** menu item and press ENTER. The Device Configuration Menu screen displays.

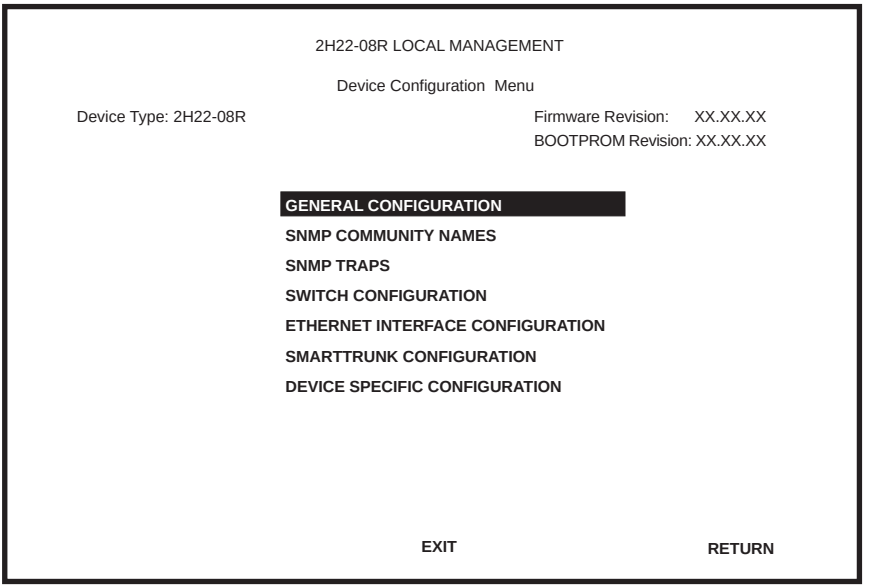


Figure 5-8 Device Configuration Menu Screen

The following briefly explains each screen accessible from the Device Configuration Menu screen:

GENERAL CONFIGURATION

The General Configuration screen allows you to monitor and configure operating parameters for the 2H22-08R. For details, refer to Section 5.7.

SNMP COMMUNITY NAMES

The SNMP Community Names screen allows you to enter new, change, or review the community names used as access passwords for device management operation. Access is dependent on a user's password level. For details, refer to Section 5.8.

SNMP TRAPS

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 5.9.

SWITCH CONFIGURATION

The Switch Configuration screen provides the basic setup options for making a switch operational in the network. For details, refer to Section 5.10.

ETHERNET INTERFACE CONFIGURATION

The Ethernet Interface Configuration screen indicates the link status, current and desired operational mode, and advertised ability for ports 1 through 8 on the 2H22-08R. Refer to Section 5.11 for details.

SMARTTRUNK CONFIGURATION

The SmartTrunk Configuration screen allows the user to logically group interfaces together to aggregate high speed uplinks. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

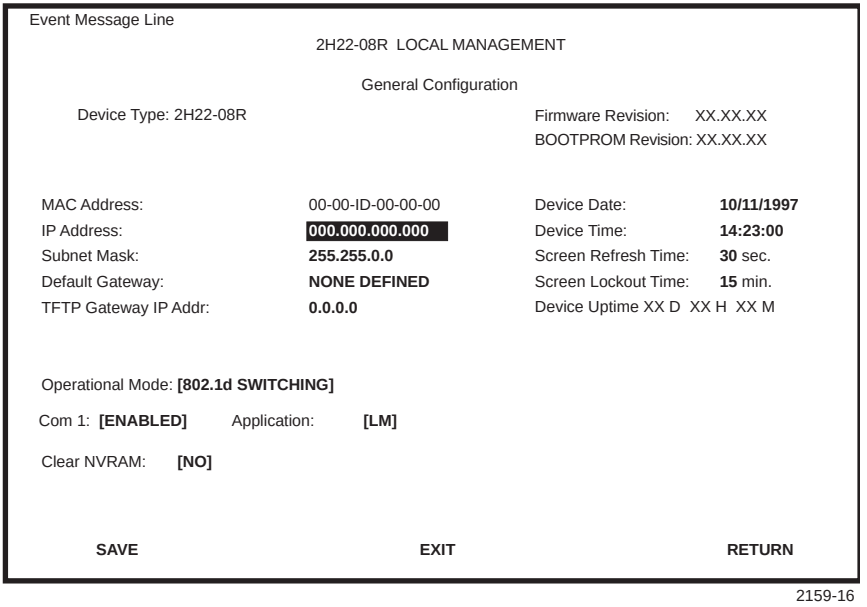
DEVICE SPECIFIC CONFIGURATION

The Device Specific Configuration menu screen allows you to select screens to configure ports or check system resources specific to the 2H22-08R. For details, refer to Section 5.12.

5.7 GENERAL CONFIGURATION SCREEN

The General Configuration screen, Figure 5-9, allows you to configure the system date and time, IP address and Subnet Mask, Default Gateway, TFTP Gateway IP address, and COM port.

To access the General Configuration screen from the Device Configuration Menu screen, use the arrow keys to highlight the **GENERAL CONFIGURATION** menu item and press ENTER. The General Configuration screen displays.



2159-16

Figure 5-9 General Configuration Screen

The following briefly explains each General Configuration screen field:

MAC Address (Read-Only)
Displays the physical address of the 2H22-08R.

IP Address (Modifiable)
Displays and allows you to set the IP address for the 2H22-08R. To set the IP address, refer to Section 5.7.1. The IP address can also be set through Runtime IP Address Discovery as previously described in Section 1.3.3.

Subnet Mask (Modifiable)
Displays the subnet mask for the 2H22-08R. A subnet mask "masks out" the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. For details about how to change the Subnet Mask from its default value, refer to Section 5.7.2.

Default Gateway (Modifiable)
Displays the default gateway for the 2H22-08R. This field is not defined until an appropriate value is entered. For details about setting the default gateway, refer to Section 5.7.3.

TFTP Gateway IP Addr (Modifiable)
Displays and allows you to set the TFTP Gateway IP address for the 2H22-08R. To set the TFTP Gateway IP address, refer to Section 5.7.4.

Device Date (Modifiable)
Contains a value that the 2H22-08R recognizes as the current date. To set a new device date, refer to Section 5.7.5.

Device Time (Modifiable)
Contains a value that the device recognizes as the current time. To enter a new time, refer to Section 5.7.6.

Screen Refresh Time (Modifiable)
Contains the rate at which the screens are updated. This setting determines how frequently (in seconds) information is updated on the screen. To enter a new update time, refer to Section 5.7.7.

Screen Lockout Time (Modifiable)
Contains the maximum number of minutes that the Local Management application displays a standalone device's screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, you have up to five minutes to respond to each of the specified standalone device's Local Management screens. In this example, after five minutes of "idleness" (no input or action), the terminal "beeps" five times, the Local Management application terminates the session, and the display returns to the Password screen. To enter a new lockout time, refer to Section 5.7.8.

Device Uptime (Read-Only)
Displays the total time that the device has been operating.

Operational Mode (Modifiable)
This field allows the user to set the 2H22-08R to operate as a traditional switch (802.1d SWITCHING option), an IEEE 802.1Q switch (802.1Q SWITCHING option), or as a Cabletron Systems SecureFast switch (SECURE FAST VLAN option).

In 802.1d SWITCHING mode, the six ports located on the front panel, and each Fast Ethernet Interface Module are bridged to each other.

In 802.1Q SWITCHING mode, the 2H22-08R is able to increase switching functionality by creating and maintaining IEEE port based VLANs.

When the operational mode is set to SECURE FAST VLAN, the 2H22-08R interfaces act as SecureFast switches. With the Cabletron Systems VLAN Manager software, the devices are able to increase their switching functionality by creating and maintaining Virtual LANs (VLANs).

For details on how to select the Operational Mode, refer to Section 5.7.9.

Com (Modifiable)
This field allows you to enable or disable the COM port. The selection toggles between ENABLED and DISABLED. The default is ENABLED. For details about setting up the COM port, refer to Section 5.7.10.

Application (Modifiable)
Displays the application set for the COM port. This field allows you to set the application that the COM port supports, which includes:

- Local Management (LM) via a terminal or modem connection
- Uninterruptible Power Supply (UPS)

The UPS setting allows you to set the COM port to monitor an American Power Conversion Uninterruptible Power Supply (UPS). For UPS, the baud rate is automatically set to 2400.

The baud rate setting for LM is automatically sensed.

For details about configuring the COM port for various applications, refer to Section 5.7.10.

Clear NVRAM (Toggle)
This allows you to reset NVRAM to the factory default settings. All user-entered parameters, such as IP address and Community Names are then replaced with 2H22-08R factory default configuration settings. For details, refer to Section 5.7.11.

5.7.1 Setting the IP Address

To set the IP address, perform the following steps:

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address in this field using Decimal Dotted Notation (DDN) format.

   For example: 134.141.79.120
3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP address field. If the entry is not valid, the Event Message Line displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-10 displays.

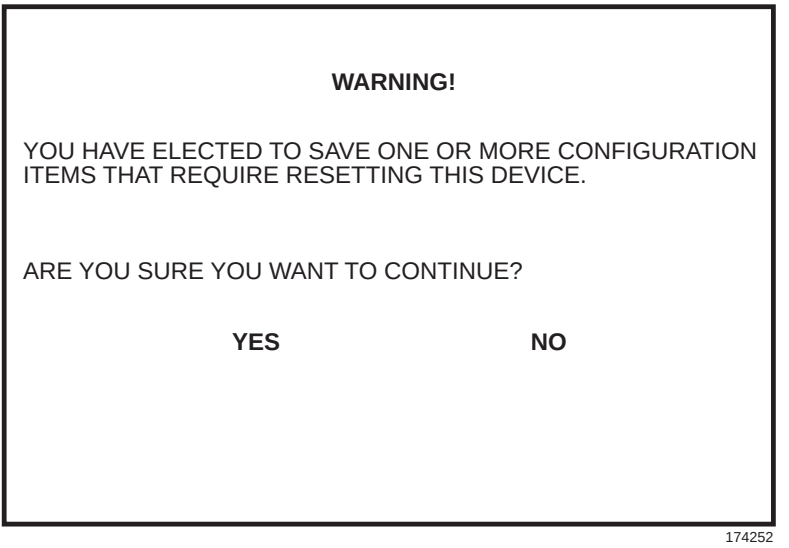


Figure 5-10 Configuration Warning Screen

5. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.7.2 Setting the Subnet Mask

If the management workstation that is to receive SNMP traps from the 2H22-08R and it is located on a separate subnet, the subnet mask for the 2H22-08R must be changed from its default.

To change the subnet mask from its default, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Decimal Dotted Notation (DDN) format.

   For example: 255.255.255.0

3. Press ENTER. If the subnet mask entry is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the screen displays the message “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-10 displays.

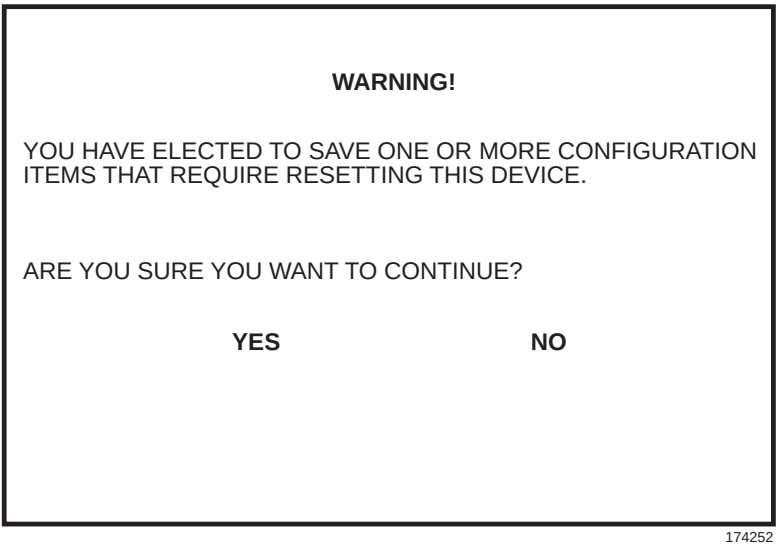


Figure 5-11 Configuration Warning Screen

5. Use the arrow keys to highlight the YES command and press ENTER. The changes are saved and the module reboots.

5.7.3 Setting the Default Gateway

If the SNMP management station is located on a different IP subnet than the 2H22-08R, a default gateway must be specified. When a SNMP Trap is generated, the 2H22-08R sends the Trap to the default gateway. To set the default gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.
2. Enter the IP address of the default gateway using the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If the default gateway entered is a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry is not valid, the screen displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Default Gateway field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The message “SAVED OK” displays at the top of the screen.

5.7.4 Setting the TFTP Gateway IP Address

If the network TFTP server is located on a different IP subnet than the 2H22-08R, a Gateway IP address must be specified. To set the TFTP Gateway IP address, perform the following steps:

1. Use the arrow keys to highlight the **TFTP Gateway IP Address** field.
2. Enter the IP address of the TFTP gateway using the DDN format.

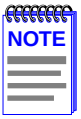
   For example: 134.141.80.122
3. Press ENTER. If the TFTP gateway IP address entered is in a valid format, the cursor returns to the beginning of the TFTP Gateway IP Address field. If the entry is not valid, the screen displays “INVALID TFTP GATEWAY IP ADDRESS OR FORMAT ENTERED”. In this instance, Local Management refreshes the TFTP Gateway IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

5.7.5 Setting the Device Date

The 2H22-08R is year 2000 compliant so that the Device Date field can be set beyond the year 1999.

To set the system date, perform the following steps:

1. Use the arrow keys to highlight the **Device Date** field.
2. Enter the date in an MM/DD/YYYY format.



It is not necessary to add separators between month, day, and year numbers, as long as each entry has the correct number of numeric characters. For example, to set the date to 03/17/1997, type “03171997” in the Device Date field.

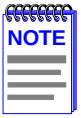
3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered is in a valid format, the message displays “SAVED OK” at the top of the screen. If the entry is not valid, Local Management refreshes the TFTP Gateway IP Address field with the previous value.

5.7.6 Setting the Device Time

To set the device clock, perform the following steps:

1. Use the arrow keys to highlight the **Device Time** field.
2. Enter the time in a 24-hour format, HH:MM:SS.



When entering the time in the system time field, separators between hours, minutes, and seconds are not needed as long as each entry uses two numeric characters. For example, to set the time to 6:45 A.M., type “064500” in the Device Time field.

3. Press ENTER to set the system clock to the time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is a valid format, the message displays “SAVED OK” at the top of the screen. If the entry is not valid, Local Management does not alter the current value and refreshes the Device Time field with the previous value.

5.7.7 Entering a New Screen Refresh Time

The screen refresh time is set between 3 and 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the message “SAVED OK” displays at the top of the screen. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

5.7.8 Setting the Screen Lockout Time

The screen lockout time is set between 1 and 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minute range, the message “SAVED OK” displays at the top of the screen. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

5.7.9 Setting the Operational Mode

If the device is configured to operate as a SecureFast switch, it must be assign and save a unique IP address (i.e., the device has rebooted and the new IP address is active) before setting the operational mode. Refer to Section 5.7.1 for more information on how to assign and save an IP address.

To set the Operational Mode, proceed as follows:

1. Use the arrow keys to highlight the **Operational Mode** field.
2. Press the SPACE bar to step to the appropriate operational mode (**802.1d SWITCHING**, **802.1Q SWITCHING**, or **SECURE FAST VLAN**).
3. Use the arrow keys to highlight the **SAVE** command and then press ENTER. The warning screen shown in Figure 5-12 displays.

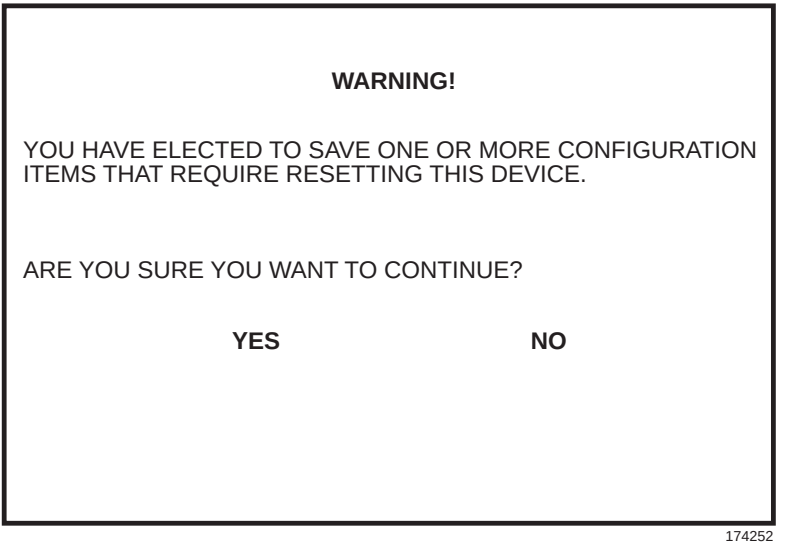
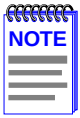


Figure 5-12 Configuration Warning Screen

4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.



Upon saving the new Operational Mode, the module reboots.

If the 2H22-08R has been set to 802.1Q SWITCHING, refer to your Port Based VLAN User's Guide to configure the devices for this type of operation.

If the 2H22-08R has been set to SECURE FAST VLAN, refer to your SecureFast documentation set to configure the devices for this type of operation.

5.7.10 Configuring the COM Port

Upon power up, the COM port is configured to the default settings of **ENABLED** and **LM**.

Before altering the COM port settings, read this entire COM port configuration section. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session.

To configure the COM port, you must enable/disable the COM port and select an application.

The 2H22-08R COM port supports the following applications:

- Local Management connections
- American Power Conversion Uninterruptible Power Supply (UPS) connections

1. Use the arrow keys to highlight the **Com** field.

Do **NOT** disable or alter the settings of the COM port while operating the current Local Management connection through a terminal. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session. If the 2H22-08R was previously assigned a valid IP address, reenter Local Management by establishing a Telnet connection to the device. If the device does not have a valid IP address and the COM port has been disabled or the settings changed, reset NVRAM on the 2H22-08R (refer to Section 5.7.11) to reestablish COM port communications.

2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**. **ENABLED** allows the COM port to be connected to the terminal and used for a particular application. **DISABLED** disallows the COM port connection to the terminal.

If the COM port is reconfigured without a valid IP address set on the device, the message shown in Figure 5-13 displays. Do not continue unless the outcome of the action is fully understood.

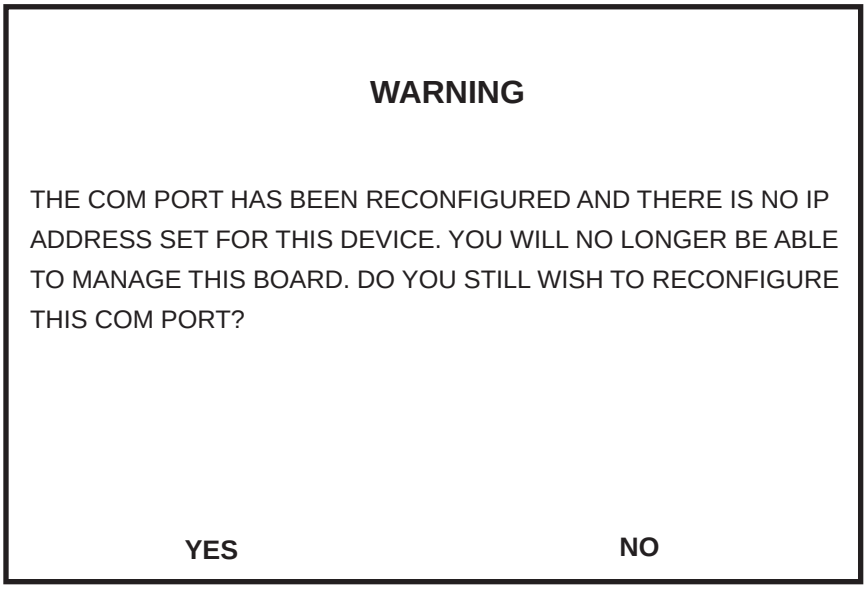


Figure 5-13 COM Port Warning Screen

3. Use the arrow keys to highlight **YES**. Press ENTER.
4. If you **ENABLED** the port, proceed to step 5. If you **DISABLED** the port, use the arrow keys to highlight **SAVE** at the bottom of the screen, then press ENTER.
5. When the message "SAVED OK" displays, the edits you made are saved.

Exiting without saving causes the message "NOT SAVED -- PRESS SAVE TO KEEP CHANGES" to display. Exiting without saving causes all edits to be lost.

6. Use the arrows keys to highlight the **Application** field.
7. Use the SPACE bar or BACKSPACE to step through the available settings until the operation you require displays. Table 5-3 lists the available settings and their corresponding applications.

Table 5-3 COM Port Application Settings

Setting	Application
[LM]	Local Management Session
[UPS]	APC Power Supply SNMP Proxy

8. Press ENTER to accept the application.
9. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen, then press the ENTER key.
10. When the message “SAVED OK” displays, the edits are saved.

5.7.11 Clearing NVRAM

Clearing NVRAM results in the loss of all user-entered parameters. Do not proceed until the following procedure is completely understood.

Clearing NVRAM enables you to clear all user-entered parameters, such as the IP address and Community Names from NVRAM.

Clear NVRAM as follows:

1. Use the arrow keys to highlight the **Clear NVRAM** field.
2. Use the SPACE bar to toggle the field to **YES**.
3. Use the arrow keys to highlight **SAVE** at the bottom of the screen.
4. Press ENTER. The warning shown in Figure 5-14 displays.

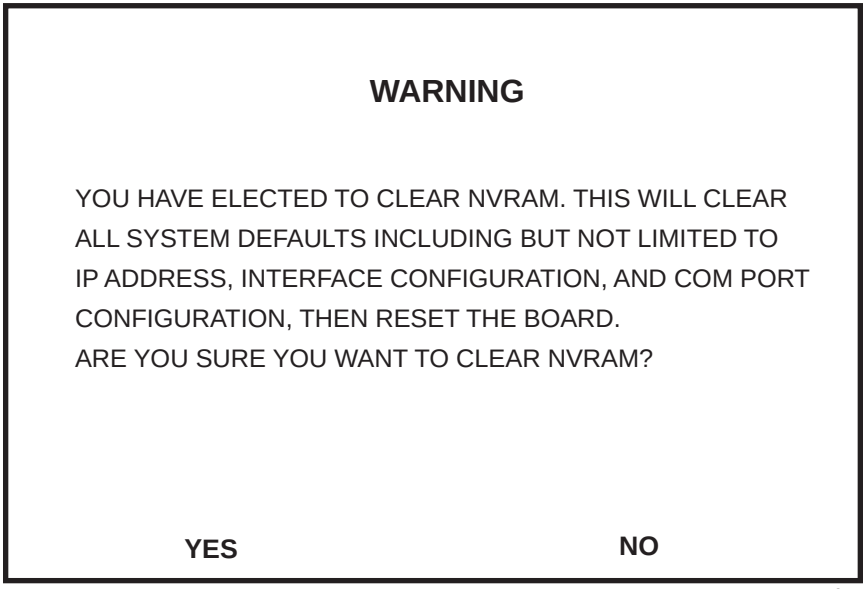


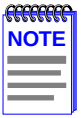
Figure 5-14 Clear NVRAM Warning Screen

5. Select **YES** and the message “CLEARING NVRAM. REBOOT IN PROGRESS...” displays.
6. The 2H22-08R clears NVRAM and reboots. All user-entered parameters default to factory settings.

5.8 SNMP COMMUNITY NAMES SCREEN

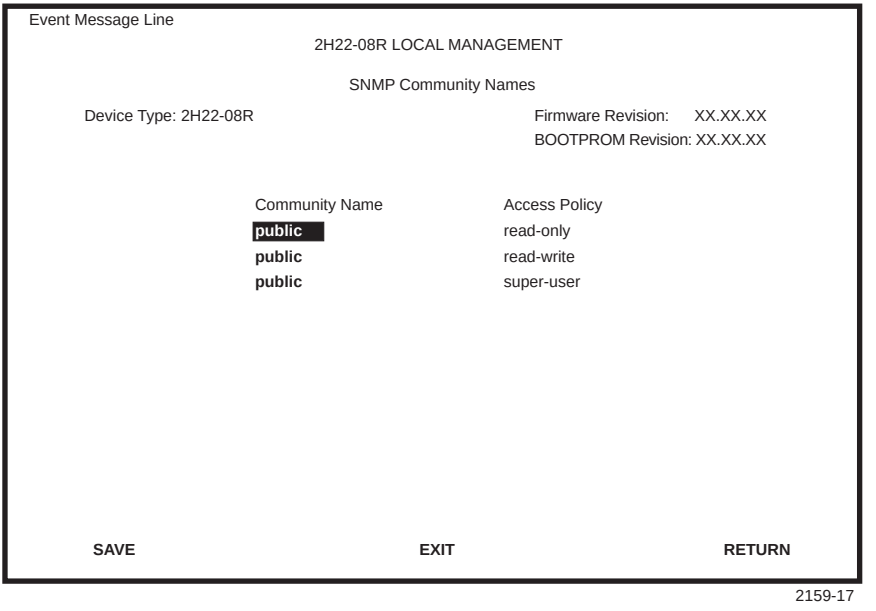
The SNMP Community Names screen allows you to set SNMP management community names. Community names act as passwords to Local/Remote Management and are agents of security access to the 2H22-08R.

Access to the 2H22-08R is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).



Super-user access gives you full management privileges, allows existing passwords to be changed, and all modifiable MIB objects for the Cabletron Container MIB and Internet MIB-II to be edited.

To access the SNMP Community Names screen from the Device Configuration Menu screen, use the arrow keys to highlight the **SNMP COMMUNITY NAMES** menu item and press ENTER. The SNMP Community Names screen, shown in Figure 5-15, displays.



2159-17

Figure 5-15 SNMP Community Names Screen

The following explains each SNMP Community Names screen field:

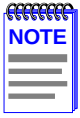
Community Name (Modifiable)
Displays the user-defined name through which a user accesses the 2H22-08R SNMP Management. Any Community Name assigned here acts as a password to Local/Remote Management. To enter a community name, refer to Section 5.8.1.

Access Policy (Read-Only)
Indicates the access accorded each Community Name. The available access levels are as follows:

read-only	This Community Name gives you read-only access to the 2H22-08R MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.
read-write	This Community Name gives you read-write access to the 2H22-08R MIB objects, excluding security protected fields for Super-User access only.
super-user	This Community Name gives you read-write access to the 2H22-08R MIB objects and allows you to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

5.8.1 Establishing Community Names

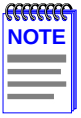
The password used to access Local Management on the Password Screen must have super-user access to view and edit the SNMP Community Names screen. Using a password with read-only or read-write access does not allow a user to view or edit the SNMP Community Names screen.



Any community name assigned in the SNMP Community Names screen is a password to its corresponding level of access to Local Management. The community name assigned super-user access is the only one that gives the user complete access to Local Management.

To establish Community Names, proceed as follows:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 31 characters).
3. Press ENTER.
4. Repeat steps 1 through 3 to modify the other community names.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The message "SAVED OK" displays. The Community Names are saved to memory and their access modes implemented.



Exiting without saving causes a "NOT SAVED?" message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

5.9 SNMP TRAPS SCREEN

Since the 2H22-08R is a SNMP compliant device, it can send messages to multiple Network Management Stations to alert users of status changes. The SNMP Traps screen is shown in Figure 5-16.

To access the SNMP Traps screen from the Device Configuration Menu screen, use the arrow keys to highlight the **SNMP TRAPS** menu item and press ENTER. The SNMP Traps screen displays.

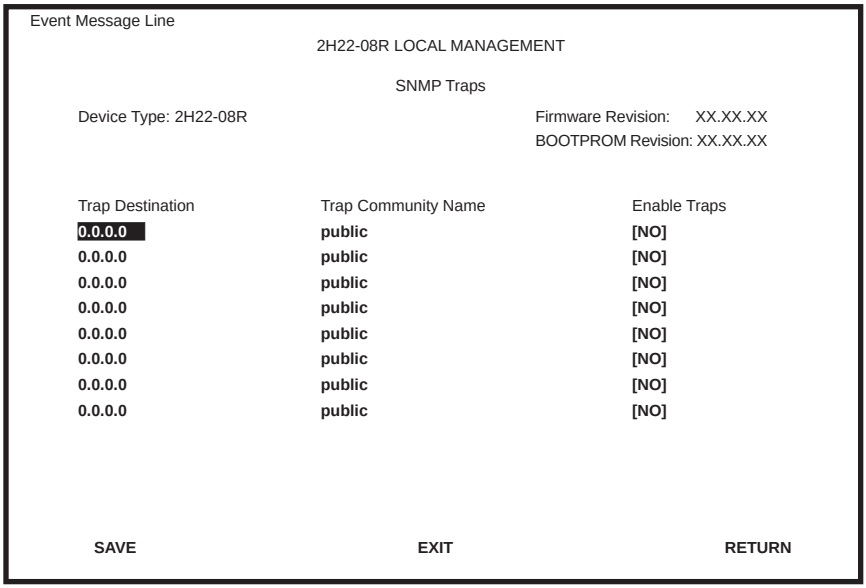


Figure 5-16 SNMP Traps Screen

The following explains each field of the SNMP Traps screen.

Trap Destination (Modifiable)
Indicates the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined as described in Section 5.9.1.

Trap Community Name (Modifiable)
Indicates the Community Name included in the trap message sent to the Network Management Station with the associated IP address to change the community name, refer to Section 5.9.1.

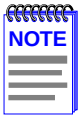
Enable Traps (Toggle)
Allows transmission of the traps to the network management station with the associated IP address. This field toggles between YES and NO as described in Section 5.9.1.

5.9.1 Configuring the Trap Table

To configure the Trap table, proceed as follows:

1. Use the arrow keys to highlight the appropriate **Trap Destination** field.
2. Enter the IP address of the workstation that is to receive traps. IP address entries must follow the DDN format.

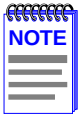
   For example: 134.141.79.121
3. Press ENTER. If an invalid entry is entered, the message “INVALID IP ENTERED” displays.
4. Use the arrow keys to highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Use the arrow keys to highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the 2H22-08R to the workstation), or **NO** (prevent alarms from being sent).
7. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays.



Exiting without saving causes a “NOT SAVED?” message to appear above the **SAVE** command. Edits are lost if they are not saved before exiting.

The designated workstations now receive traps from the 2H22-08R.

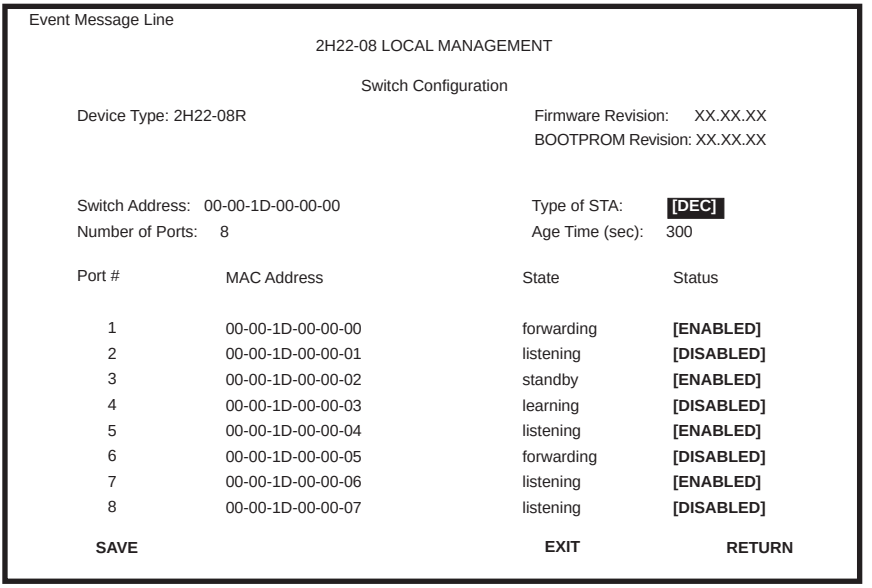
5.10 SWITCH CONFIGURATION SCREEN



The Switch Configuration Screen will not be available if the operational mode of the device has been set to SECURE FAST VLAN. This screen may only be used by devices configured to operate as 802.1D or 802.1Q switches.

The Switch Configuration screen, Figure 5-17, provides the basic setup options to make a switch operational in your network.

To access the Switch Configuration screen from the Device Configuration Menu screen, use the arrow keys to highlight the **SWITCH CONFIGURATION** menu item and press ENTER. The Switch Configuration screen displays showing Ports 1 through 8.



2159-19

Figure 5-17 Switch Configuration Screen

The following describes each field of the Switch Configuration screen:

Switch Address (Read-Only)
Displays the MAC address of the switch.

Number of Ports (Read-Only)
Displays the total number of switched ports.

Type of STA (Toggle)
Allows you to set the method that switches use to decide which switch is the controlling (Root) switch when two or more switches exist in parallel (Spanning Tree Algorithm). Valid entries include IEEE, DEC, and None. To set the STA, refer to Section 5.10.1.

Age Time (Modifiable)
Allows the user to set the amount of time (in seconds) the 2H22-08R keeps an address in its switch table before discarding it. The device discards an address from its switch table if it does not receive a valid Bridge Protocol Data Unit (BPDU) from the applicable address in the amount of time specified in the Age Time field. To change the Age Time field from the default value of 300 seconds, refer to Section 5.10.2.

Port # (Read-Only)
Lists each switch port on the 2H22-08R. If the number of ports is greater than eight, then the additional ports are listed on subsequent screens.

MAC Address (Read-Only)
Displays the hardware address assigned to each listed port.

State (Read-Only)
There are five states that can display in this field. These states are described as follows:

Disabled: Management disabled this interface. No traffic is received or forwarded while the interface is disabled.

Learning: The switch in Learning State is looking at Bridge Protocol Data Units (BPDUs) to determine the current network topology (during start-up or after being deleted), or when the Spanning Tree Algorithm detects a network topology change.

Listening: The switch is not adding information to the Transparent Database. The switch is monitoring BPDU traffic while preparing to move from the learning to the forwarding state.

Forwarding: The switch is operating and this interface is forwarding traffic.

Standby: This interface does not forward any traffic through the switch because a loop condition is detected by the STA.

Status (Toggle)
Allows you to disable or enable a port by setting the status of the listed interface to either ENABLED or DISABLED. To set the port status, refer to Section 5.10.3.

5.10.1 Setting the STA

The Spanning Tree Algorithm (STA) setting allows you to set the method that the switches use to decide which is the controller (Root) switch when two or more switches are in parallel. The available selections are IEEE, DEC, and NONE.

To set the STA, proceed as follows:

1. Use the arrow keys to highlight the **Type of STA** field.
2. Use the SPACE bar to step to the appropriate setting of **IEEE**, **DEC**, or **NONE**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.

4. Press ENTER. The message “SAVED OK” displays.

5.10.2 Setting the Age Time

To set the Age Time, proceed as follows:

1. Use the arrow keys to highlight the **Age Time** field.
2. Enter the desired Age Time in increments of 10. The available Age Time range is 10 seconds to 1,000,000 seconds with the default value being 300 seconds.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

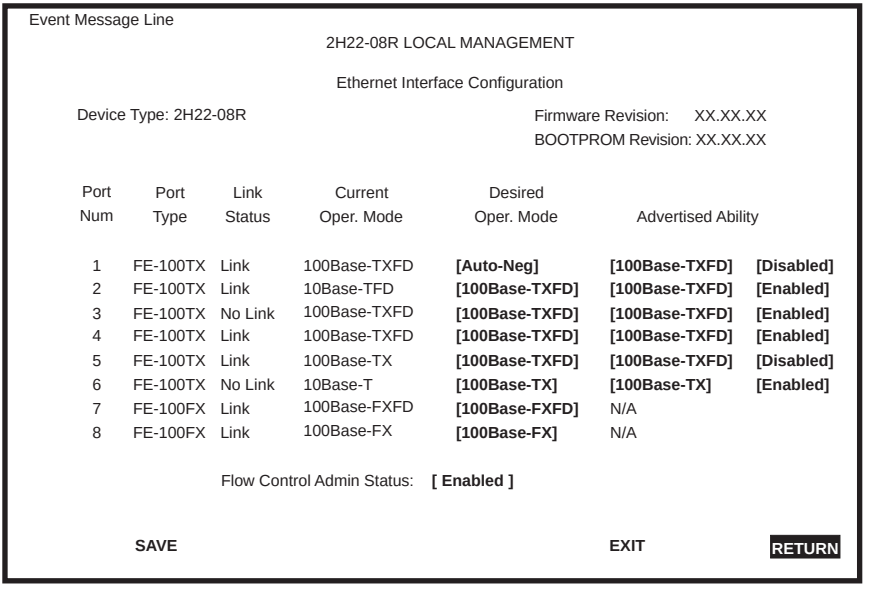
5.10.3 Setting (Enabling or Disabling) the Port Status

To set the status of an interface (port), proceed as follows:

1. Use the arrow keys to highlight the **Status** field of the port.
2. Use the SPACE bar to toggle to either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.11 ETHERNET INTERFACE CONFIGURATION

To access the Ethernet Interface Configuration Menu screen shown in Figure 5-18 from the Device Configuration Menu screen, use the arrow keys to highlight the **ETHERNET INTERFACE CONFIGURATION** menu item, and press ENTER. The Ethernet Interface Configuration screen displays.



2159-23

Figure 5-18 Ethernet Interface Configuration Screen

The following section briefly explains each field of the Ethernet Interface Configuration screen:

Port Type (Read-Only)
Displays the type of physical media supported by ports 1 through 8.

Link Status (Read-Only)
Indicates whether or not there is a physical connection from a particular port to another 10BASE-T, 100BASE-TX/FX, or 100BASE-TXFD/FXFD device. One of the following values displays:

- **Link –** There is a link signal present and a valid physical connection to another 10BASE-T, 100BASE-TX/FX, or 100BASE-TXFD/FXFD device.
- **No Link –** There is no link signal present and there is no valid physical connection to another device.

Current Oper. Mode (Read-only)
This field displays the current operating mode of a port. Depending on the interface installed (100BASE-FX, 100BASE-F3, or 100BASE-TX), this field displays the following:

- 100Base-TX interface – Auto-Neg, Unknown (if there is no Link), 10Base-T, 10Base-TFD (full duplex), 100Base-TX, or 100Base-TXFD (full duplex).
- 100BASE-FX interface – Unknown (if there is no Link), 100Base-FX or 100Base-FXFD (full duplex).

Desired Oper. Mode (Selectable)
This field allows you to select the desired operational mode for an interface.

- FE-100TX Interface – The field steps to **Auto-Neg**, **10Base-T**, **10Base-TFD** (full duplex), **100Base-TX**, and **100Base-TXFD** (full duplex). In normal operation, the port with an FE-100TX interface is capable of auto-negotiating the operational mode and no further user setup is required. Section 5.11.1 describes how to configure an FE-100TX.
- FE-100FX/F3 Interface – The field toggles between **100Base-FX** or **100Base-FXFD** (full duplex) operation. Section 5.11.4 describes configuring a port with an FE-100FX or FE-100F3 interface.

In normal operation, the installed FE-100TX port automatically establishes a link with the device at the other end of the segment without requiring user setup. However, Local Management allows you to optionally configure that port.

Advertised Ability (Selectable)
During auto-negotiation, the FE-100TX sends information about its capability to the device at the other end of the segment. The capabilities of a port with an FE-100TX installed are 10BASE-T, 10BASE-TFD (full duplex mode), 100BASE-TX and 100BASE-TXFD (full duplex mode). In normal operation, with all capabilities enabled, the FE-100TX "advertises" that it has the ability to operate in any mode. The Network Manager may choose to set up the port so that only a portion of the available capabilities are advertised and the others are disabled. For example, only 100BASE-TX and 100BASE-TXFD might be enabled so that only devices that operate at 100 Mbps can communicate with that port. Section 5.11.3 describes how to enable or disable advertised modes.

Flow Control Admin Status (Selectable)
This setting controls whether or not the switch will send a jam out all ports when there is too much traffic for the switch to process. The jam will clear the ports and enable the switch to process the current frame information. It will enable the optional ports, 7 and 8, to continue to pass traffic, giving those two ports priority. Section 5.11.3 describes the how to enable or disable advertised modes.

5.11.1 Configuring an FE-100TX Interface

In normal operation, a port with an FE-100TX interface automatically establishes a link with the device at the other end of the segment and no user setup is required. Section 5.11.2 and Section 5.11.3 provide instructions for manually configuring the port with an FE-100TX installed.

5.11.2 Setting the FE-100TX Operational Mode

Use this field to set the active technology. This field steps to Auto-Negotiation, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex). If Auto-Negotiation is selected, the FE-100TX automatically sets the active technology. To manually set the active technology through Local Management, proceed as follows:

1. Use the arrow keys to highlight the **Desired Oper. Mode** field.
2. Use the SPACE bar to select the desired mode. Press ENTER. If any mode other than Auto-Negotiation is selected, the port only operates in the chosen mode and auto-negotiation is disabled.
3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "SAVED OK" displays and Local Management saves the changes to memory. The selected mode displays in both the Desired Oper. Mode field and the Current Oper. Mode field.

5.11.3 Setting the FE-100TX Advertised Ability

During normal operation, ports 1 through 6 and optionally in port 7 or 8 an FE-100TX auto-negotiates to the highest speed possible. Under some circumstances, the Network Administrator may want the port to advertise only some of the available modes and not operate in other modes. This field steps to **10Base-T**, **10Base-TFD** (full duplex), **100Base-TX**, and **100Base-TXFD** (full duplex). To set the advertised ability, proceed as follows:

1. Use the arrow keys to highlight the **Advertised Ability** field.
2. Use the SPACE bar to select the desired mode.
3. Use the LEFT-ARROW key to move back to the **Advertised Ability** selection and use the SPACE bar to select the next mode to enable or disable.
4. Use the RIGHT-ARROW key to move across to the **Enabled/Disabled** field to the right of the selection.
5. Use the SPACE bar to select **Enabled** or **Disabled**. Press ENTER. Continue this process until you have completed enabling or disabling the advertised modes.

6. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory.

5.11.4 Configuring an FE-100FX or FE-100F3 Interface for Port 7 or 8

When an FE-100FX or FE-100F3 is installed in port 7 or 8, it must be manually set to operate in the same technology as the device at the other end of the connected segment. Section 5.11.5 provides instructions for manually setting the port with an FE-100FX or FE-100F3 interface.

5.11.5 Setting the FE-100FX and FE-100F3 in Operational Mode

Use this field to set the active technology. This field toggles between **100Base-FX** and **100Base-FXFD** (full duplex). To set the active technology through Local Management, proceed as follows:

1. Use the arrow keys to highlight the **Desired Operational Mode** field.
2. Use the SPACE bar to select **100Base-FX** or **100Base-FXFD** (full duplex).
3. Press ENTER. The port now operates in the chosen mode.
4. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory.

5.11.6 Setting the Flow Control Admin Status

This field toggles between ENABLED and DISABLED. To enable or disable Flow Control, do the following:

1. Use the arrow keys to highlight the **Flow Control Admin Status** field.
2. Use the SPACE bar to toggle the field to the desired setting. Press ENTER.
3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory.

5.12 DEVICE SPECIFIC CONFIGURATION MENU

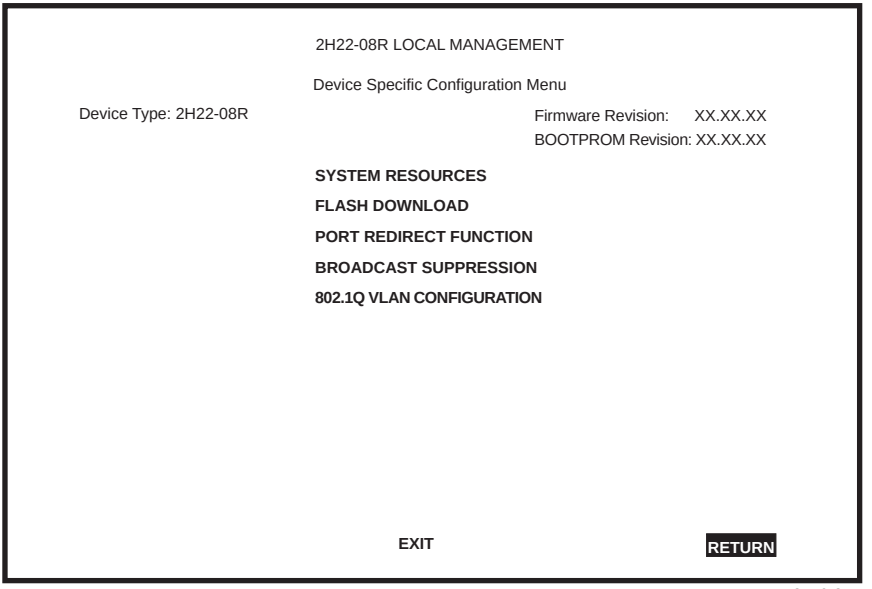
The Device Specific Configuration Menu screen allows you to select from four screens to configure ports or check system resources specific to the 2H22-08R.

NOTE

The PORT REDIRECT FUNCTION and BROADCAST SUPPRESSION menu items on the Device Specific Configuration Menu screen will not display if the operational mode of the device has been set to SECUREFAST VLAN:

Section 5.7.9 provides instructions for setting the operational mode.

To access the Device Specific Configuration menu screen from the Device Configuration Menu screen, use the arrow keys to highlight the **DEVICE SPECIFIC CONFIGURATION** menu item and press ENTER. The Device Specific Configuration Menu screen, shown in Figure 5-19, displays.



2159-21

Figure 5-19 Device Specific Configuration Menu Screen

The following explains each field of the Device Specific Configuration Menu screen:

SYSTEM RESOURCES

The System Resources screen displays the amount of FLASH memory, DRAM, and NVRAM installed, indicates the amount of available memory and provides information on 2H22-08R operation. For details, refer to Section 5.13.

FLASH DOWNLOAD

The FLASH Download screen allows you to download information from FLASH memory and force the 2H22-08R to download a new image file from a TFTP server. For details, refer to Section 5.14.

PORT REDIRECT FUNCTION

The Port Redirect Function screen allows you to redirect traffic from one or multiple ports to a specific destination switch port. For details refer to Section 5.15.

BROADCAST SUPPRESSION

The Broadcast Suppression screen allows you to set a desired limit of receive broadcast frames that is forwarded per port per second. For more details, refer to Section 5.16.

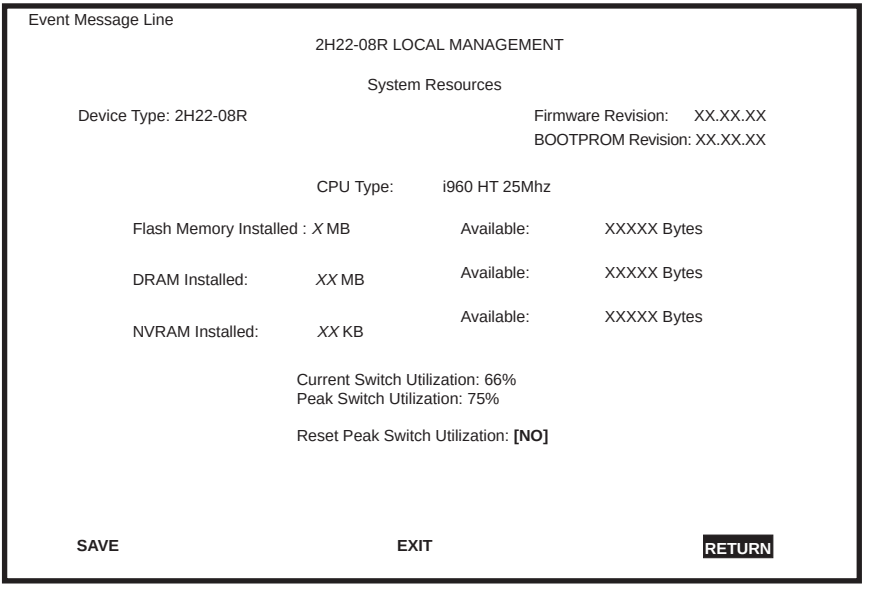
802.1Q VLAN CONFIGURATION

This menu item only displays when you select **802.1Q SWITCHING** from the Operational Mode field in the General Configuration screen. Refer to Section 5.7.9 for information on setting the Operational Mode field. Refer to the *Port Based VLAN User's Guide* for more information on VLAN configuration and the Local Management screens accessed through the 802.1Q VLAN CONFIGURATION menu item.

5.13 SYSTEM RESOURCES SCREEN

The System Resources screen, Figure 5-20, provides information concerning the processor used in the 2H22-08R and the amount of FLASH memory, DRAM, and NVRAM that is installed and how much of that memory is available. This screen also allows you to monitor the current processor (switch) utilization and the peak switch utilization.

To access the System Resources screen from the Device Specific Configuration Menu screen, use the arrow keys to highlight the **SYSTEM RESOURCES** menu item and press ENTER. The System Resources screen displays.



2159-40

Figure 5-20 System Resources Screen

The following briefly explains each field on the System Resources screen.

CPU Type (Read-only)
Indicates the microprocessor used in the 2H22-08R.

Flash Memory Installed (Read-only)
Indicates the amount of FLASH memory installed in the 2H22-08R and how much is currently available.

DRAM Installed (Read-only)
Indicates the amount of DRAM installed in the 2H22-08R and how much is currently available.

NVRAM Installed (Read-only)
Indicates the amount of NVRAM installed in the 2H22-08R and how much of it is currently available.

Current Switch Utilization (Read-only)
Shows the percentage of the device's switching capacity currently being used.

Peak Switch Utilization (Read-only)
Shows the peak percentage of device's switching capacity used, since the last reset.

Reset Peak Switch Utilization (Toggle)
Allows you to reset the Peak Switch Utilization field. The switch may be set to either YES or NO as described in Section 5.13.1. YES resets the Peak Switch Utilization field to the current system traffic.

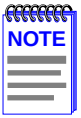
5.13.1 Setting the Reset Peak Utilization

To set the Reset Peak Utilization field to YES or NO, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak Switch Utilization** field.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message "SAVED OK" displays.

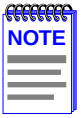
5.14 FLASH DOWNLOAD SCREEN

The Flash Download screen, shown in Figure 5-21, allows you to upgrade the device with a different operating image.



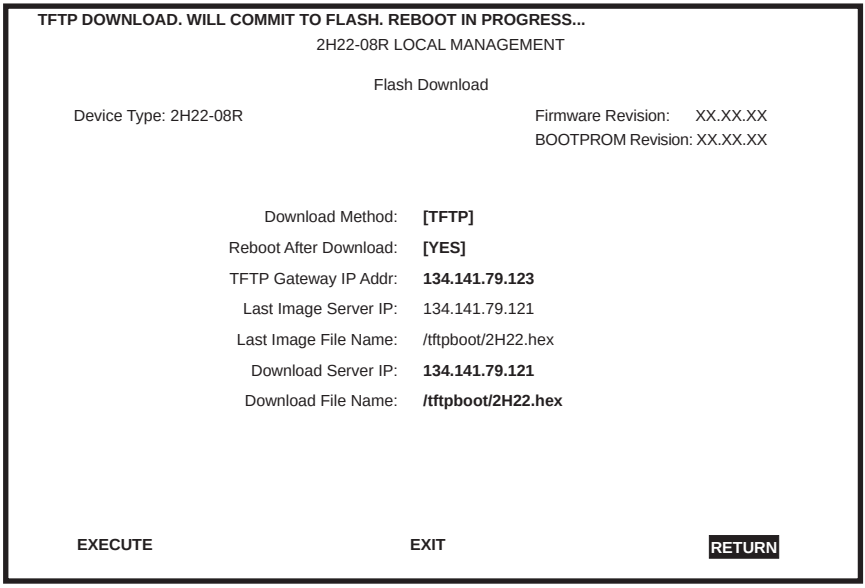
You may also force the download of an image by changing the position of Switch 6 located inside the device. Refer to Section C.2.1, **Setting the Mode Switch**, for details.

Before downloading a new image to the 2H22-08R, load the image onto the network TFTP server.



For information on how to setup a workstation as a TFTP server, refer to the specific workstation documentation.

To access the Flash Download screen from the Device Specific Configuration Menu screen, use the arrow keys to highlight the **FLASH DOWNLOAD** menu item and press ENTER. The Flash Download screen displays.



2159-24

Figure 5-21 Flash Download Screen

NOTE

Download Server IP and Download Server File Name displays only when TFTP or RUNTIME are selected in Download Method.

The following briefly explains each field of the Flash Download screen:

Download Method (Selectable)
This field steps to **BOOTP**, **TFTP**, and **RUNTIME**. If set for BOOTP, the 2H22-08R sends out a BootP request to determine the IP address of the TFTP server and the File Name of the image to be downloaded. If set for TFTP or RUNTIME, the 2H22-08R attempts a TFTP download based on the IP address and filename entered in the fields at the bottom of the Flash Download screen. Section 5.14.1 describes downloading using BootP. Section 5.14.2 describes how to download using TFTP. Section 5.14.3 describes downloading using RUNTIME.

Reboot After Download (Modifiable only when **RUNTIME** is chosen)
This field notifies you that the 2H22-08R reboots after the download is complete. If a RUNTIME Download is performed, this field toggles between YES and NO. If YES is selected, the 2H22-08R reboots after the download completes. If NO is selected, the device continues using the existing the firmware image and stores the new firmware image in FLASH memory. When the device is reset or during the next power-up, the device boots from FLASH memory using the new image.

TFTP Gateway IP Addr (Selectable)
This field shows the IP address of the TFTP gateway server defined in the General Configuration screen in Section 5.7.4.

Last Image Server IP (Read-only)
This field shows the IP address of the server used for the previous FLASH Download.

Last Image File Name (Read-only)
This field shows the complete path and file name of the last image downloaded to FLASH.

If TFTP or RUNTIME are selected as the download method (see Figure 5-21), the following two additional fields display:

Download Server IP (Selectable)
Enter the IP address of the TFTP server to be used for the FLASH download.

Download File Name (Selectable)
Enter the complete TFTP Server path and file name of the new image in this field.

5.14.1 Image File Download Using BootP

To download a firmware image into FLASH using BootP, proceed as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **BOOTP**.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway server (this defaults to the same IP address set in the TFTP Gateway IP Addr field in the General Configuration screen).
5. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message “BOOTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS...” displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.14.2 Image File Download Using TFTP

To download a firmware image into FLASH using TFTP, proceed as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **TFTP**.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway server (this defaults to the same IP address set in the TFTP Gateway IP Addr field on the General Configuration screen).
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the TFTP server using the DDN format. For example: 134.141.79.121
7. Use the arrow keys to highlight the **Download File Name** field.

8. Enter the complete pathway and file name of the image stored on the download server. For example: /tftpboot/2H22.hex

9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "TFTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS..." displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.14.3 Image File Download Using RUNTIME

To download a firmware image into FLASH using RUNTIME, proceed as follows:

1. Use the arrow keys to highlight the **Download Method** field.

2. Use the SPACE bar to select **RUNTIME**.

3. Use the arrow keys to highlight the **Reboot After Download** field.

4. Use the SPACE bar to select either **YES** or **NO**. Select **YES** if you want the device to reboot after the download is completed. Select **NO** if you want the device to store the new image in FLASH memory until the device is reset during the next power-up.

5. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.

6. Set the IP address of the TFTP gateway server (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).

7. Use the arrow keys to highlight the **Download Server IP** field.

8. Enter the IP address of the TFTP server using the DDN format. For example: 134.141.79.121

9. Use the arrow keys to highlight the **Download File Name** field.

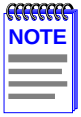
10. Enter the complete pathway and file name of the image stored on the download server.

    For example: /tftpboot/2H22.fls

11. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "RUNTIME DOWNLOAD. WILL

COMMIT TO FLASH." displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

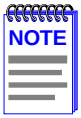
5.15 PORT REDIRECT FUNCTION SCREEN



The Port Redirect Function screen is only used if the operational mode of the device has been set to **802.1d SWITCHING**. Refer to Section 5.7.9, **Setting the Operational Mode** for instructions on configuring the device to operate in this mode.

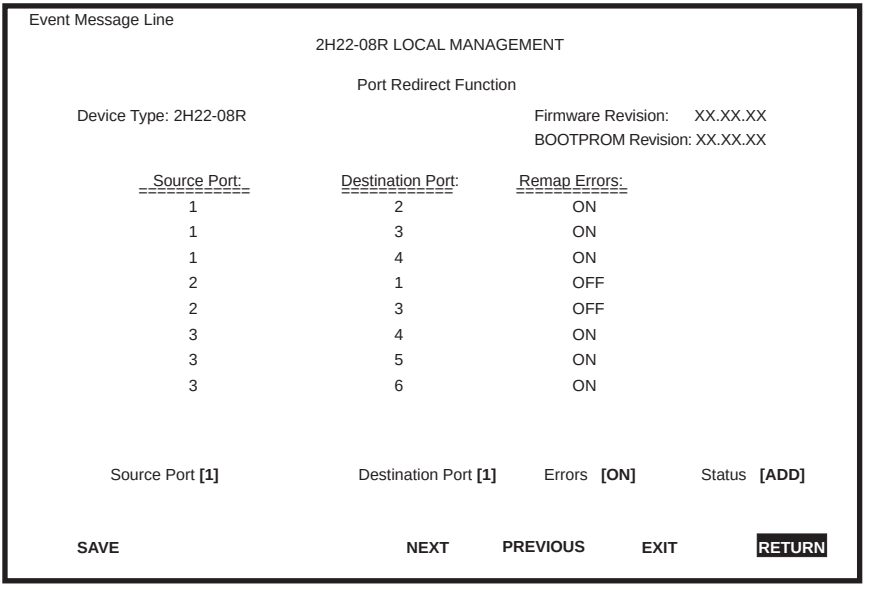
The Port Redirect Function screen, Figure 5-22, allows you to set each interface as a source or destination interface on the 2H22-08R. An interface can be set to have one or more destination interfaces. For example, interface 1 can be set as a source interface with three destinations, interfaces 2, 3, and 4. Traffic from interface 1 is then automatically redirected to interfaces 2, 3, and 4. Interface 1 can also serve as a destination interface for other ports.

The port redirect function is extremely useful for troubleshooting purposes, as it enables traffic to be sent to a particular interface(s) where, with the use of an analyzer or RMON probe, all current traffic from the source interface(s) can be examined.



Although all traffic from the source port (including, if desired, error frames) is sent to the destination port, normal switching is still performed for all frames on the source port.

To access the Port Redirect Function screen from the Device Specific Configuration Menu screen use the arrow keys to highlight the **PORT REDIRECT FUNCTION** menu item and press ENTER. The Port Redirect Function screen displays.



1960_22

Figure 5-22 Port Redirect Function Screen

The following definitions briefly explain each field of the Port Redirect Function screen:

Source Port (Read-only)
Shows which ports are currently set as source ports as described in Section 5.15.1.

Destination Port (Read-only)
Shows which ports are currently set as destination ports as described in Section 5.15.1.

Remap Errors (Read-only)
Displays whether the corresponding source ports are configured to send errored frames to the destination ports, or to drop all errored frames before forwarding traffic as described in Section 5.15.3.

Source Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a source port as described in Section 5.15.1.

Destination Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a destination port as described in Section 5.15.2.

Errors (Toggle)
Allows the user to configure the source ports to either send errored frames to selected destination ports, or to drop errored frames, and send only valid traffic to the destination ports. The default setting of this field is [ON], refer to Section 5.15.1 and Section 5.15.2 for more information about setting this field.

Status (Selectable)
Allows you to add or delete the source and destination ports selected in the Source Port [n] and Destination Port [n] fields as described in Section 5.15.2.

5.15.1 Displaying the Source and Destination Entries

There can be more than one Port Redirect Function screen depending on the number of port redirect entries. Each screen displays up to ten port redirect entries. If there is more than one screen of redirect entries, the **NEXT** and/or **PREVIOUS** command displays at the bottom of the screen, allowing the user to navigate to either the next or previous screen.

For example, with three screens of entries, the **NEXT** command is displayed at the bottom of the first screen. In the second screen, the **NEXT** and **PREVIOUS** commands displays. In the last screen, only the **PREVIOUS** command displays.

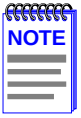
To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER and the next screen of entries is displayed.

To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries in the previous screen.

5.15.2 Changing Source and Destination Ports

Add or delete source port and destination port entries as follows:

1. Use the arrow keys to highlight the **Source Port** field.
2. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number displays.
3. Use the arrow keys to highlight the **Destination Port** field.
4. Use the SPACE bar or BACKSPACE to step to the appropriate port number for the destination port.
5. Use the arrow keys to highlight the **Status** field.
6. Use the SPACE bar to select either the **[ADD]** or **[DEL]** (delete) option. Press ENTER. This adds or deletes the port selections made in steps 2 and 4 and also updates the screen Source Port and Destination Port list.
7. Use the arrow keys to highlight the **Errors** field.
8. Use the SPACE bar to select either the **[ON]** or **[OFF]** option and press ENTER. **[ON]** forces the source device and port to forward errored frames to the destination device(s) and port(s). **[OFF]** forces the errored to be dropped before forwarding traffic.



If more than one port is to be redirected, repeat steps 1 through 8 for each additional setting, then go to step 9 to save all the new settings at once.

9. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message “SAVED OK” displays. This saves the new settings and updates the Source Interface and Destination Interface read-only fields.

5.15.3 Changing the Remap Errors Field

To prevent errored frames from being sent to the destination ports, perform the following:

1. Use the arrow keys to highlight the **[OFF]** selection, next to the Errors field at the bottom of the screen, and press ENTER.
2. Use the arrow keys to highlight the **SAVE** command and press ENTER. The changes are saved to memory.

To return to the default setting of [ON], which enables the errored frames to be sent to the destination ports, perform the following:

1. Use the arrow keys to highlight the **[ON]** selection, next to the Errors field at the bottom of the screen, and press ENTER.
2. Use the arrow keys to highlight the **SAVE** command and press ENTER. The changes are saved to memory.

5.16 BROADCAST SUPPRESSION SCREEN

The Broadcast Suppression screen, Figure 5-23, allows you to set a desired limit of receive broadcast frames that are switched out to the other interfaces.

NOTES

The Broadcast Suppression screen will not be available if the operational mode of the device has been set to SECURE FAST VLAN. This screen may only be used by devices configured to operate as traditional or 802.1Q switches.

Broadcast frames received above the threshold setting are dropped.

To access the Broadcast Suppression screen from the Device Specific Configuration menu screen, use the arrow keys to highlight the **BROADCAST SUPPRESSION** menu item and press ENTER. The Broadcast Suppression screen displays.

Event Message Line

2H22-08R LOCAL MANAGEMENT

Broadcast Suppression

Device Type: 2H22-08R

Firmware Revision: XX.XX.XX

BOOTPROM Revision: XX.XX.XX

PORT #	Total RX	Peak Rate	Time Since Peak	Threshold	Reset Peak
1	12345678910	150000	999:23:59	**150000**	**[NO]**
2	12345678910	150000	999:23:59	**150000**	**[NO]**
3	12345678910	150000	999:23:59	**150000**	**[NO]**
4	12345678910	150000	999:23:59	**150000**	**[NO]**
5	12345678910	150000	999:23:59	**150000**	**[NO]**
6	12345678910	150000	999:23:59	**150000**	**[NO]**
7	12345678910	150000	999:23:59	**150000**	**[NO]**
8	12345678910	150000	999:23:59	**150000**	**[NO]**

SAVE **EXIT** **RETURN**

2159-25

Figure 5-23 Broadcast Suppression Screen

The following explains each field of the Broadcast Suppression screen:

PORT # (Read-only)
Identifies the number of the port.

Total RX (Read-Only)
Displays the total number of broadcast frames received.

Peak Rate (Read-Only)
Displays the highest number of broadcast frames received in a one-second interval.

Time Since Peak (Read-Only)
Displays the time since peak rate was achieved.

Threshold (Modifiable)
Allows you to set the desired limit of receive broadcast frames that are forwarded per port per second. To set the threshold, refer to Section 5.16.1.

Reset Peak (Modifiable)
Allows you to reset the peak rate. Resetting the Peak Rate also resets the Time Since Peak field. The Reset Peak field toggles between YES and NO. To set the Reset Peak field, refer to Section 5.16.2.

5.16.1 Setting the Threshold

To set the Threshold, proceed as follows:

1. Use the arrow keys to highlight the **Threshold** field for the selected port.
2. Type in the numbers for the desired limit. Only enter values in increments of ten (for example; 10, 20, 30, etc.).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.16.2 Setting the Reset Peak

To set the Reset Peak field to **YES** or **NO**, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak** field for the selected port.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrows keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays and the Time Since Peak field is also reset.

5.17 DEVICE STATISTICS MENU SCREEN

NOTE

The SWITCH STATISTICS menu item on the Device Statistics Menu screen will not display if the operational mode of the device has been set to SECURE FAST VLAN.

Section 5.7.9 provides instructions on setting the operational mode.

The Device Statistics Menu screen, Figure 5-24, provides access to screens that allow you to obtain switch statistics about frame traffic through each interface and view operating statistics about each port.

To access the Device Statistics Menu from the Device Menu screen, use the arrow keys to highlight the **DEVICE STATISTICS** menu item and press ENTER. The Device Statistics Menu screen displays.

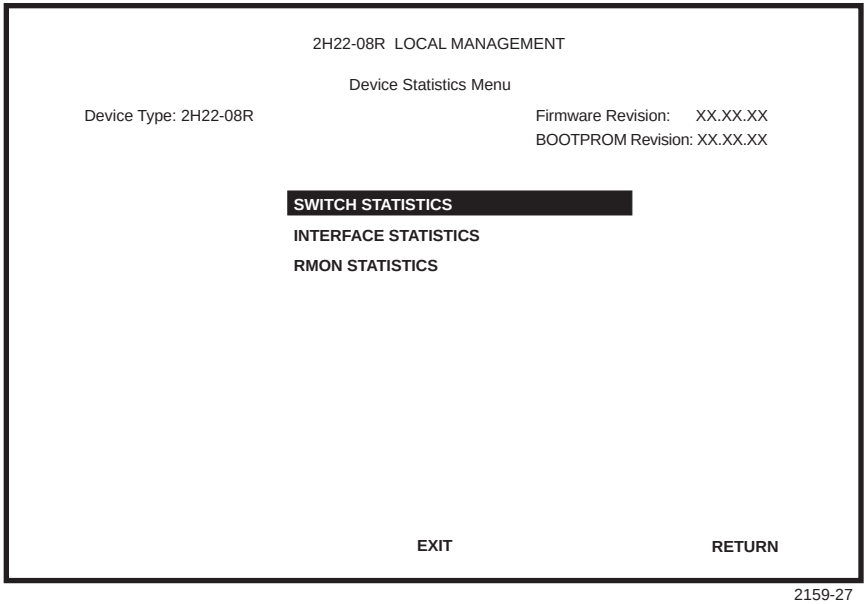


Figure 5-24 Device Statistics Menu Screen

The Device Statistics Menu screen displays the following menu items:

SWITCH STATISTICS

The Switch Statistics screen lists the number of frames received, transmitted, filtered, and forwarded by each interface.

INTERFACE STATISTICS

The Interface Statistics screen provides the MIB-II statistics for each switched interface, on an interface-by-interface basis.

RMON STATISTICS

The RMON Statistics screen displays all the statistics gathered by the embedded RMON agent built into the 2H22-08R.

5.18 SWITCH STATISTICS SCREEN

The Switch Statistics screen, Figure 5-25, lists the number of frames received, transmitted, filtered, and forwarded by each port.

NOTE

The Switch Statistics screen will not be available if the operational mode of the device has been set to SECURE FAST VLAN. This screen may only be used by devices configured to operate as traditional or 802.1Q switches.

To access the Switch Statistics screen from the Device Statistics Menu screen, use the arrow keys to highlight the **SWITCH STATISTICS** menu item and press ENTER. The Switch Statistics screen displays.

2H22-08R LOCAL MANAGEMENT

Switch Statistics

Device Type: 2H22-08R

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

Port #	Frames Rcvd	Frames Txmtd	Frames Fltrd	Frames Frwded
1	100	100	0	100
2	100	100	0	100
3	100	100	0	100
4	100	100	0	100
5	100	100	0	100
6	100	100	0	100
7	100	100	0	100
8	100	100	0	100

CLEAR COUNTERS EXIT RETURN

2159-28

Figure 5-25 Switch Statistics Screen

The Switch Statistics screen displays the following fields:

Port # (Read-Only)
Identifies the port number.

Frames Rcvd (Read-Only)
Displays the number of frames received by the port since the last power-up or reset.

Frames Txmtd (Read-Only)
Displays the number of frames transmitted by the port since the last power-up or reset.

Frames Fltrd (Read-Only)
Displays the number of frames filtered by the port since the last power-up or reset.

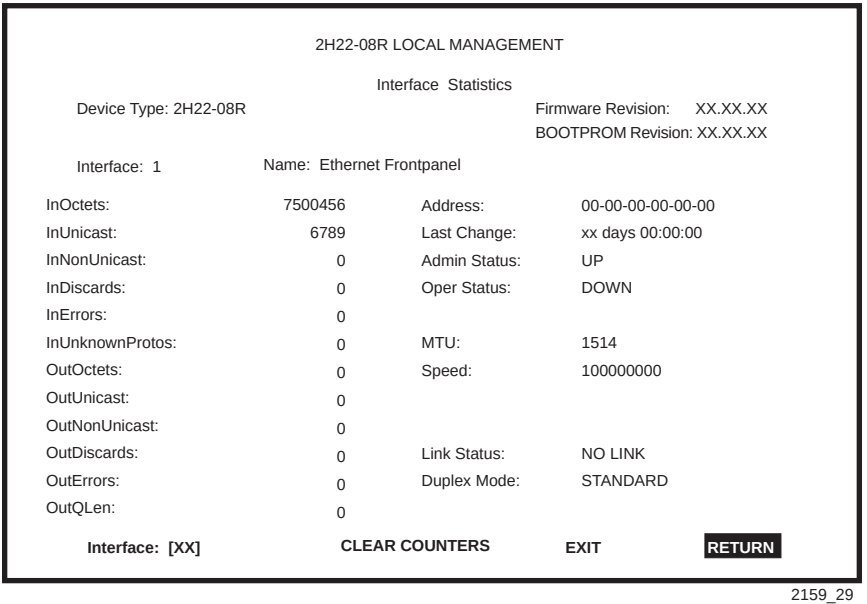
Frames Frwded (Read-Only)
Displays the number of frames forwarded by the port.

CLEAR COUNTERS (Command)
This command clears all the counters of the ports displayed to zero. To clear the counters, use the arrow keys to highlight **CLEAR COUNTERS** at the bottom of the screen, then press ENTER.

5.19 INTERFACE STATISTICS SCREEN

The Interface Statistics screen is used to gather MIB-II statistics for all of the 2H22-08R interfaces (ports 1 through 6 and Fast Ethernet Interface Modules).

To access the Interface Statistics screen, use the arrow keys to highlight the **INTERFACE STATISTICS** menu item on the Device Statistics Menu screen and press ENTER. The Interface Statistics screen, Figure 5-26, displays.



2159_29

Figure 5-26 Interface Statistics Screen

The following definitions explain each field of the Interface Statistics screen:

Interface (Read-only)
This field displays the Interface number for which statistics are currently being displayed. Figure 5-26 shows the Interface field displaying 1. This represents port 1 of the 2H22-08R. To view other interface statistics, refer to Section 5.19.1.

Name (Read-only)
The Name field displays the type of interface for which statistics are being displayed.

InOctets (Read-only)
This field displays the total number of octets (bytes) that have been received on the Interface. This includes all octets from bad frames, and Frame Check Sequence (FCS) octets.

InUnicast (Read-only)
The InUnicast field displays the total number of packets that have been received that were sent to a single address.

InNonUnicast (Read-only)
This field displays the total number of packets that have been received that were delivered to a broadcast or multicast address.

InDiscards (Read-only)
The InDiscards field displays the total number of inbound packets that were discarded, even though the packets contained no errors. This field may increment because the switch needed to free up buffer space, or the switch was being overutilized.

InErrors (Read-only)
This field displays the total number of inbound packets that have been discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

InUnknownProtos (Read-only)
The InUnknownProtos field displays the total number of packets that were discarded because the packets were in an unknown, or unsupported, format.

OutOctets (Read-only)
This field displays the total number of octets (bytes) that have been transmitted from the Interface. This includes all Frame Check Sequence (FCS) octets.

OutUnicast (Read-only)
The OutUnicast field displays the total number of packets transmitted that were sent to a single address.

OutNonUnicast (Read-only)
This field displays the total number of packets transmitted to a broadcast or multicast address.

OutDiscards (Read-only)
The OutDiscards field displays the total number of outbound packets that were discarded, even though the packets contained no errors. This field may increment, because the switch needed to free up buffer space, or the switch was being overutilized.

OutErrors (Read-only)
This field displays the total number of outbound packets discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

OutQLen (Read-only)
The OutQLen field displays the length of the packet queue. The field represents the number of packets in the queue.

Address (Read-only)
This field displays the MAC Address of the interface that is currently being displayed.

Last Change (Read-only)
This field displays the last time that the interface was reset.

Admin Status (Read-only)
This field displays the current status of the interface. If this field displays “Testing”, no packets may be passed on this interface.

Oper Status (Read-only)
This field displays the current status of the interface. If this field displays "Testing", no packets may be passed on this interface.

MTU (Read-only)
The MTU field displays the maximum frame size (in octets) that a packet may contain to be received or transmitted from this interface.

Speed (Read-only)
The Speed field displays an estimate of the interface's current bandwidth in bits per second.

Link Status (Read-only)
This field displays the current link status of the interface. This field will read either "Link" or "No Link".

Duplex Mode (Read-only)
This field indicates whether the interface is operating in normal or full duplex mode. This field will read either "Standard" or "Full Duplex".

Interface [XX] (Command)
This command is used to enter an interface number for viewing statistics. For instructions on how to use this command, refer to Section 5.19.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.19.2.

5.19.1 Displaying Interface Statistics

To display the statistics for any interface, proceed as follows:

1. Use the arrow keys to highlight the **Interface [XX]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL (delete) key to decrement) the interface number.
3. Press ENTER (neither the **Interface #** fields nor the statistics will change until ENTER is pressed).

5.19.2 Using the Clear Counters Command

To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command.
2. Press ENTER, the counters for the selected interface are reset to zero.

5.20 RMON STATISTICS SCREEN

RMON statistics for each interface, on an interface-by-interface basis, are viewed through the RMON Statistics screen shown in Figure 5-27.

Access the RMON Statistics screen by using the arrow keys to highlight the **RMON STATISTICS** field on the Device Statistics Menu screen and pressing ENTER. The RMON Statistics screen displays.

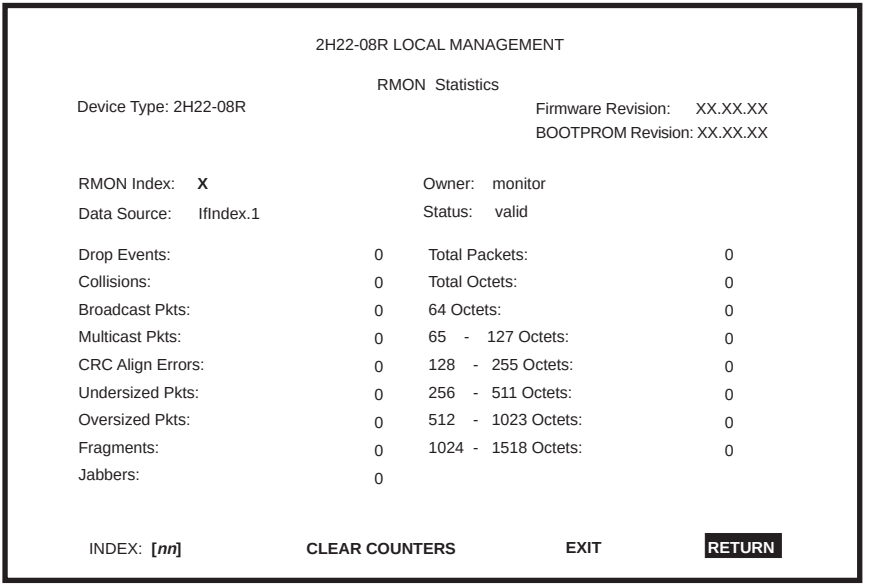


Figure 5-27 RMON Statistics Screen

The following definitions explain each field of the RMON Statistics screen:

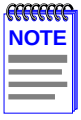
RMON Index (Read-only)
This field displays the current Ethernet interface for which statistics are being shown. The 2H22-08R has an embedded RMON agent that gathers statistics for each of its interfaces.

Data Source (Read-only)
This field displays the source of the statistics data that is currently being displayed on the screen. Figure 5-27 shows that the data source for this RMON index is Interface 1 by displaying the name IfIndex.1. If the screen was displaying RMON statistics for Interface 4, the name displayed would be IfIndex.4.

Owner (Read-only)
This field displays the name of the entity that last configured the device.

Status (Read-only)
The Status field displays the current operating status of the displayed interface. This field displays “valid” or “invalid”.

Drop Events (Read-only)
This field displays the total number of times that the RMON agent was forced to discard packets due to the lack of available switch resources.



The Drop Events field does not display the number of packets dropped, it only displays the number of times that the RMON agent was forced to discard packets.

Collisions (Read-only)
This field displays the total number of collisions that have occurred on this interface.

Broadcast Pkts (Read-only)
The Broadcast Pkts field displays the total number of good packets that were directed to the broadcast address. The value of this field does not include multicast packets.

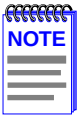
Multicast Pkts (Read-only)
The Multicasts field displays the total number of good packets received that were directed to a multicast address. The value of this field does not include packets directed to the broadcast address.

CRC Align Errors (Read-only)
This field displays the number of packets with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data packet that ensures that the data received is the same as the data that was originally sent. Alignment errors are due to packets not sent to higher level protocols in the correct order.

Undersized Pkts (Read-only)
The Undersized Pkts field displays the number of packets received with a valid CRC and whose size was less than the minimum Ethernet frame size of 64 bytes (not including preamble).

Oversized Pkts (Read-only)
The Oversized Pkts field displays the number of packets received with a valid CRC and whose size exceeded 1518 data bytes (not including preamble).

Fragments (Read-only)
This field displays the number of received packets with less than the minimum number of bytes, or received packets, were less than 64 bytes (excluding framing bits), but including Frame Check Sequence (FCS) bytes) that had a bad FCS, and an invalid CRC.



It is normal for the Fragments field to increment. This is because the RMON agent increments the field when runts are detected (which are normal occurrences due to collisions) and when noise hits occur.

Jabbers (Read-only)
This field displays the total number of packets that were greater than 1518 bytes and had either a bad FCS or a bad CRC.

Total Packets (Read-only)
This field displays the total number of packets (including bad packets, broadcast packets, and multicast packets) received on this interface.

Total Octets (Read-only)
This field displays the total number of octets (bytes) of data, including those in bad packets, received on this interface.

64 Octets (Read-only)
Displays the total number of packets including bad packets, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).

65 – 127 Octets (Read-only)
Displays the total number of packets, including bad packets, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).

128 – 255 Octets (Read-only)
Displays the total number of packets, including bad packets, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).

256 – 511 Octets (Read-only)
Displays the total number of packets, including bad packets, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).

512 – 1023 Octets (Read-only)
Displays the total number of packets, including bad packets, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).

1024 – 1518 Octets (Read-only)
Displays the total number of packets, including bad packets, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including FCS bytes).

Index [*nn*] (Command)
This command is used to enter an index number for viewing statistics. For instructions on how to use this command, refer to Section 5.20.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.20.2.

5.20.1 Displaying RMON Statistics

To display the statistics for any index, proceed as follows:

1. Use the arrow keys to highlight the **Index [*nn*]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL (delete) key to decrement) the index number.
3. Press ENTER (neither the **RMON Index:** field nor the statistics will change until ENTER is pressed).

5.20.2 Using the Clear Counters Command

To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** field.
2. Press ENTER, the counters for the selected index are reset to zero.

5.21 NETWORK TOOLS

The Network Tools function allows you to access and manage network devices. Figure 5-28 shows the Network Tools Help screen.

To access the Network Tools screen, use the arrow keys to highlight the **NETWORK TOOLS** menu item in the Device Menu screen and press ENTER. The Network Tools screen displays. Figure 5-28 displays when "help" is entered at the prompt, and lists all the commands available to you.

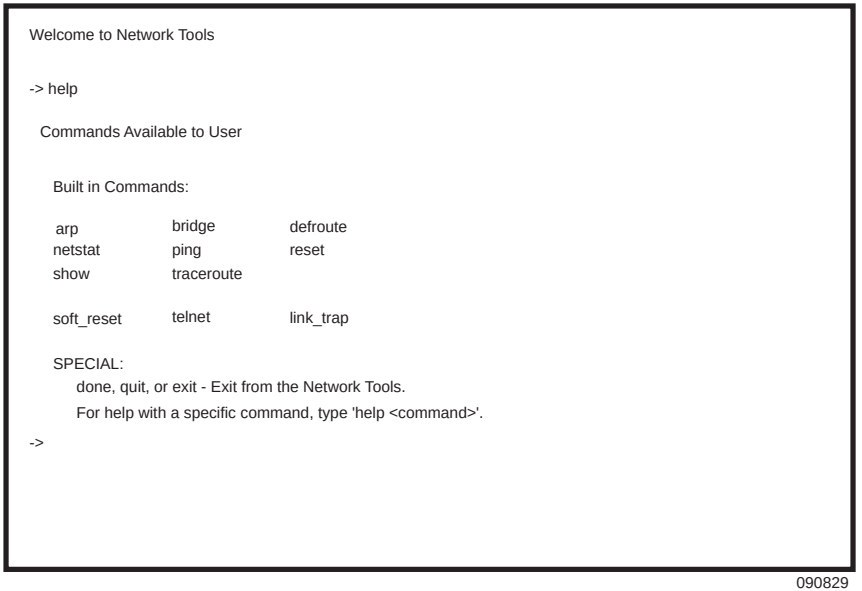
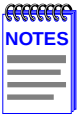


Figure 5-28 Network Tools Help Screen

The Network Tools functions are performed using a series of commands. Entering commands in Network Tools involves typing the command to be executed at the Network Tools prompt, adding any desired or required extensions, and pressing ENTER.

There are two categories of commands in the command set.

- Built-in Commands - Allow you to access and manage network devices. The commands are: **arp**, **bridge**, **defroute**, **netstat**, **ping**, **reset**, **show**, **traceroute**, **soft_reset**, **telnet**, and **link_trap**.
- Special Commands - Allow you to exit from Network Tools. The commands are **done**, **quit**, and **exit**.



The conventions used in describing the commands in Network Tools are as follows:

Arguments enclosed by [ ] are required.

Arguments enclosed by < > are optional.

In the following command examples, the information entered by user is in shown in **bold** Helvetica font.

To abort the output or interrupt a process, press the CONTROL key and c key simultaneously, designated as ^C here.

The commands are presented in the following format:

command:

Syntax:	Shows the required command format. It indicates where arguments, if any, must be specified.
Description:	Briefly describes the command and its uses.
Options:	Lists any additional fields in the appropriate format which may be added to the command.
Example:	Shows an example of the command.

5.21.1 Built-in Commands

The built-in commands listed in this section activate functions on the LM managed device or devices being accessed through Network Tools.

arp:

Syntax: arp <options>

Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

Each ARP cache entry lists the network *interface* that the device is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types are displayed as numbers, which stand for the following states:

1 - Other
2 - Invalid entry (cannot ping device, timed out, etc.)
3 - Dynamic route entry
4 - Static route entry (not subject to change)

You can specify the arp command without options, or with one of the following options:

Options:
-a Views cache data
-d Deletes an IP address entry. Requires additional arguments: <Interface Number> <IP address>
-s Adds a static entry. Requires additional arguments: <Interface Number> <IP address> <MAC address>
-f Flushes the ARP cache

Example:

```
-> arp -a
# Interface          Network Address     Physical Address    Media Type
# (SonicInt)         122.144.40.111      00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.48.109      00.00.0e.f3.3d.14   3(dynamic)
# (SonicInt)         122.144.52.68       00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.21.43       00.00.0e.03.1d.3c   3(dynamic)


-> arp -d 1 122.144.52.68


-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c


-> arp -f
```

05141-67

bridge:

Syntax: bridge [ENABLE/DISABLE] [IFNUM/ALL]

Description: The bridge command enables bridge management to be enabled or disabled at your request, either one at a time or all at once. Specifying a single interface number will affect the bridging status of that interface, while specifying ALL will affect every interface.

Options: [ENABLE/DISABLE]

[IFNUM/ALL]

Example:

```
-> bridge disable all


-> bridge enable 1


-> bridge disable 1
```

05141-68

defroute:

Syntax: defroute

Description: The defroute command allows you, in the syntax order shown above, to view, set, or delete the default IP route to a managed device through the specified interface.

Options: defroute [interface number] [IP address]

defroute delete [interface number] [IP address]

Example:

```
-> defroute 2 147.152.42.32
```

05141-69

link_trap:

Syntax: link_trap [enable/disable/status] [PORT/all]

Description: The link_trap command allows link traps to be enabled or disabled when specifying a single port, or simultaneously when specifying “all” or no ports. When one or all ports are specified to enable, disable, or find their status, their current condition is displayed.

Options: Not Applicable

Example:

```
-> link_trap status
LINK TRAP STATUS:

  Port 1  is ENABLED          Port 2  is DISABLED
  Port 3  is ENABLED          Port 4  is ENABLED

NetTools-> link_trap disable 2
Link traps have been DISABLED on port 2

NetTools-> link_trap disable all
Link traps have been DISABLED on all ports (1-24)

NetTools-> link_trap status 3
Link traps are ENABLED on port 3
```

netstat:

Syntax: netstat [options]

Description: The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.

Options: -i Displays status and capability information for each interface.
-r Displays routing information for each interface.

Example:

```
-> netstat -i
Interface + Description     MTU     Speed      Admin  Oper  MAC Addr

# 1 (ethernet -csmacd)      1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x11

-> netstat -r
Destination          Next-hop              Interface

# Default Route      DirectConnection      1
# 134.141.0.0        DirectConnection      2
# 134.141.0.0        DirectConnection      3
```

05141-70

ping:

Syntax: ping [IP address]

Description: The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Options: [IP address]

Example:

```
-> ping 122.144.40.10
122.144.40.10 is alive
```

05141-71

reset:

Syntax: reset

Description: This reset command initiates a hardware reset of the device. The reset command initializes the CPU processor, runs the onboard diagnostics, and restarts the software image, which restores your configuration settings from NVRAM. You are queried to confirm the reset command to ensure against unwanted resets.

The Network Tools connection to the device will be terminated upon execution of this command.

Options: Not Applicable

Example:

```
-> reset
```

17421-45

show:

Syntax: show <PROTOCOL> <TABLE>

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP, IPX, DECnet, and AppleTalk. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table will be displayed at the end of the table display.

Options: <protocol> IP, IPX, DECNET, Appletalk

<table> ARP, ROUTE, FIB, Server, Interface

Example:

```
-> show Appletalk interfaces

# Interface   AdminStatus   OperStatus   MTU    Forwarding   Framing
# 1           enabled       enabled      1500   enabled      ethernet
# 2           disabled      disabled     1500   disabled     ethernet


-> show IP ARP

# Interface   MediaType     PhysicalAddress     NetworkAddress
# 3           3 (dynamic)   00:00:1d:04:40:5d   123.456.40.1
# 4           3 (dynamic)   08:00:20:0e:d8:31   123.456.40.30
```

17421-46

traceroute:

Syntax: traceroute [IP address]

Description: The traceroute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Options: [IP Address]

Example:

```
-> traceroute 122.144.11.52

# next-hop[0] : 122.144.60.45
# next-hop[1] : 122.144.8.113
# next-hop[2] : 122.144.61.45
# 122.144.11.52 is alive : 3 hops away.
```

05141-77

soft-reset:

Syntax: soft-reset

Description: This command restarts the software image, which restores your configuration settings from NVRAM. You will be queried to confirm the reset command to ensure against unwanted resets.

The Network Tools connection to the device will be terminated upon execution of this command.

Options: Not Applicable

Example:

```
-> soft-reset
```

22511-76

telnet:

Syntax: telnet [IP address] [Port #]

Description: The telnet command allows you to communicate with another host (that supports Telnet connections) using the Telnet protocol. You must specify the remote host using its IP address. The [IP address] field is mandatory. If no Port number is specified, telnet will attempt to contact the host at the default port.

Options: [IP address]

[Port #]

Example:

```
-> telnet 134.141.12.345
Trying 134.141.12.345
Connected to 134.141.12.345

SunOS UNIX (server1)


login:
```

2251-77

link_trap:

Syntax: link_trap [enable/disable/status] [PORT/all]

Description: The link_trap command allows link traps to be enabled or disabled when specifying a single port, or simultaneously when specifying “all” or no ports. When one or all ports are specified to enable, disable or find their status, their current condition is displayed.

Options: Not Applicable

Example:

```
-> link_trap status 3
   Link traps are ENABLED on port 3
-> link_trap disable all
   Link traps have been DISABLED on all ports (1 through 8)
```

2364_lnktrp

5.21.2 Special Commands

done, quit, exit:

Syntax: done, quit, or exit

Description: The done, quit, or exit command allows you to exit from Network Tools and return to the Main Menu screen.

Options: Not Applicable

Example:

```
-> done

Connection closed
```

05141-72

APPENDIX A
SPECIFICATIONS

This appendix provides operating specifications for the 2H22-08R SmartSwitch 2208 standalone device. Cabletron Systems reserves the right to change these specifications at any time without notice.

A.1 DEVICE SPECIFICATIONS

Processor:	Intel i960 RISC processor
Dynamic Random Access Memory (DRAM):	16 MB
FLASH Memory:	4 MB

A.2 PHYSICAL PROPERTIES

Dimensions:	7.11H x 43.18W x 46.99D (cm) 2.8H x 17W x 18.5D (in)
Weight (Unit) 2H43-51R:	5.45 kg (12 lb)
MTBF (Predicted):	200,000 hours

A.3 ELECTRICAL SPECIFICATIONS

Line Input Range Volts (V)	Input Current Amperes (A)	Frequency Hertz (Hz)	Input Power Volt Amps (VA)
100–125 Vac	2.0 A	50/60 Hz	200 VA
200–240 Vac	1.0 A		

A.4 ENVIRONMENTAL REQUIREMENTS

Operating Temperature:	5°C to 40°C (41°F to 104°F)
Storage Temperature:	-30°C to 73°C (-22°F to 164°F)
Operating Relative Humidity:	5% to 90% (non-condensing)

A.5 INPUT/OUTPUT PORTS

Ports 1 through 6	Fast Ethernet 10/100 Mbps (100BASE-TX compliant) with RJ45 type connectors.
Slots for optional Fast Ethernet Interface Modules (ports 7 and 8)	Slots accept three types of optional Fast Ethernet Interface Modules: FE100-TX, FE100-FX, and FE100-F3.

A.6 COM PORT PINOUT ASSIGNMENTS

The COM port is a serial communications port that supports Local Management or connection to a UPS.

Table A-1 shows the COM port pin assignments.

Table A-1 COM Port Pin Assignments

Pin	Signal Name	Input/Output
1	Transmit Data (XMT)	Output
2	Data Carrier Detect (DCD)	Output
3	Data Set Ready (DSR)	Input
4	Receive Data (RCV)	Input
5	Signal Ground (GND)	NA
6	Data Terminal Ready (DTR)	Output
7	Request to Send (RTS)	Input
8	Clear to Send (CTS)	NA

A.7 REGULATORY COMPLIANCE

This equipment meets the following safety and electromagnetic compatibility (EMC) requirements:

Safety	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 73/23/EEC.
EMC	FCC Part 15, EN 55022, CSA C108.8, EN 50082-1, VCCI V-3, AS/NZS 3548 and 89/336/EEC.

APPENDIX B

FE-100TX, FE-100FX, AND FE-100F3 SPECIFICATIONS

This appendix provides specifications for the FE-100TX, FE-100FX, and FE-100F3 Fast Ethernet Interface Modules that are supported by the 2H22-08R.

B.1 FE-100TX

NOTE

The FE-100TX uses an RJ45 connector supporting Category 5 Unshielded Twisted Pair (UTP) cabling, which has an impedance of 85 to 111 ohms.

The slide switch on the FE-100TX determines the crossover status of the cable pairs. If the switch is on the **X** side, the pairs are internally crossed over. If the switch is on the **=** side, the pairs are not internally crossed over. Figure B-1 shows the pinouts for the FE-100TX in both positions.

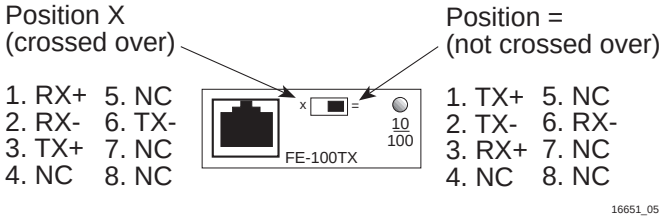


Figure B-1 FE-100TX Pinouts

B.2 FE-100FX

The FE-100FX shown in Figure B-2 uses an SC style connector that supports multimode fiber optic cabling. Specifications for the FE-100FX are listed in Table B-1, below.

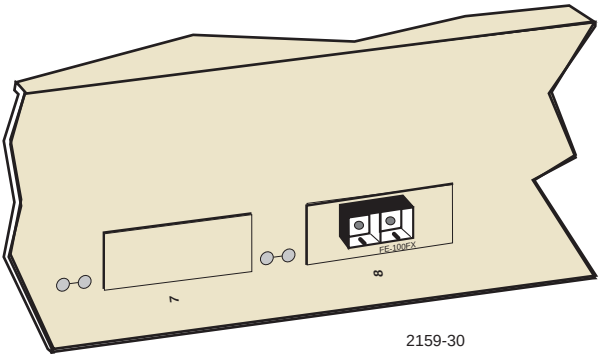


Figure B-2 FE-100FX

Table B-1 Transmitter Power

Cable Type	Worst Case Budget	Typical Budget
50/125 µm fiber optic	6.0 dB	9.0 dB
62.5/125 µm fiber optic	9.0 dB	12.0 dB
100/140 µm fiber optic	15.0 dB	18.0 dB

NOTE

The transmitter power levels and receive sensitivity levels listed are peak power levels after optical overshoot. A peak power meter must be used to correctly compare the values given above to those measured on any particular port. If power levels are being measured with an average power meter, add 3 dB to the measurement to compare the measured values to the values listed above.

B.3 FE-100F3

The FE-100F3 shown in Figure B-3 uses an SC style connector that supports single mode fiber optic cabling. Specifications for the FE-100F3 are listed in Table B-2, below.

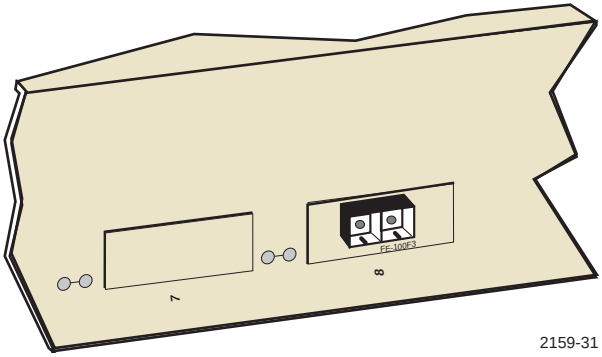


Figure B-3 FE-100F3

Table B-2 Transmitter Power

Cable Type	Worst Case Budget	Typical Budget
8/125 µm fiber optic	>10.0 dB	<10.0 dB
12.5/125 µm fiber optic	>10.0 dB	<10.0 dB

NOTE

The transmitter power levels and receive sensitivity levels listed are peak power levels after optical overshoot. A peak power meter must be used to correctly compare the values given above to those measured on any particular port. If power levels are being measured with an average power meter, add 3 dB to the measurement to compare the measured values to the values listed above.

APPENDIX C

OPTIONAL INSTALLATIONS AND MODE SWITCH BANK SETTINGS

ONLY QUALIFIED SERVICE PERSONNEL SHOULD ATTEMPT THE FOLLOWING PROCEDURES.

NUR QUALIFIEZIERTE SERVICE PERSONNAL DIE FOLGENDE PROCEDURE FOLGEN SOLLTEN.

SOLAMENTE PERSONAL CALIFICADO DEBE INTENTAR ESTE PROCEDIMIENTO.

The top cover must be removed to gain access to the mode bank switches and to install the Fast Ethernet Interface Modules.

This appendix covers the following items:

- Required tools (Section C.1)
- Removing the chassis cover (Section C.2)
- Locations, functions, and settings for the mode switches (Section C.2.1)
- Installing Optional Fast Ethernet Interface Modules (Section C.3)

C.1 REQUIRED TOOLS

You need the following tools to perform the procedures provided in this appendix:

- Antistatic wrist strap (provided)
- Phillips screwdriver

C.2 REMOVING THE CHASSIS COVER

This section describes how to remove the 2H22-08R chassis cover.

DO NOT REMOVE THE COVER FROM THE 2H22-08R WHILE POWER IS APPLIED TO THE UNIT. HAZARDOUS VOLTAGES ARE PRESENT AND COULD CAUSE PERSONAL INJURY AND/OR DAMAGE THE UNIT.

DO NOT POWER UP THE 2H22-08R AGAIN UNTIL THE COVER AND SCREWS ARE IN PLACE.

DECKEL VON DAS 2H22-08R NICHT ABZIEHEN UNTER SPANNUNG. GEFAHR FÜR DAS PERSONNAL UND/ODER DAS GERÄT WEGEN GEFÄHRLICHE SPANNUNGEN ENSTEHT.

2H22-08R NICHEINSCHALTEN SO LANG DER DECKEL UND SCHRAUBEN NICHT EINGEBAUT SIND.

NO DEBE DE REMOVER LA TAPA DURENTE QUE ESTE CONELTADO A LA CORRIENTE, UNA DESCARGA ELECTRICA LE PUEDE CAUSAR Y PROBOCARLE DAÑOS, AL IGUAL QUE AL APARATO.

NO ENCHUFE A LA CORRIENTE HASTA QUE LA TAPA Y LOS TORNILLOS ESTEN EN SU LUGAR.

CAUTION: THIS UNIT MAY HAVE MORE THAN ONE POWER SUPPLY CORD. DISCONNECT TWO POWER SUPPLY CORDS BEFORE SERVICING TO AVOID ELECTRIC SHOCK.

VORSICHT: DIESES GERÄT HAT MEHR ALS EINEN NETZANSCHLUß. TRENNEN SIE VOR WARTUNGSARBEITEN DIE 2 NET ZANSCHLÜSSE VOM NETZ, UM ELEKTRISCHE SCHLÄGE ZU VERMEIDEN.

ATTENTION: CET APPAREIL COMPORTE PLUS D'UN CORDON D'ALIMENTATION. RAFIN DE PREVENIR LES CHOCS ELECTRIQUES, DEGRANCHER LES DEUX CORDONS D'ALIMENTATION AVANT DE FAIRE LE DEPANNAGE.

To remove the chassis cover, proceed as follows:

TURN OFF THE 2H22-08R BY UNPLUGGING BOTH POWER CORDS FROM THE REAR OF THE CHASSIS.

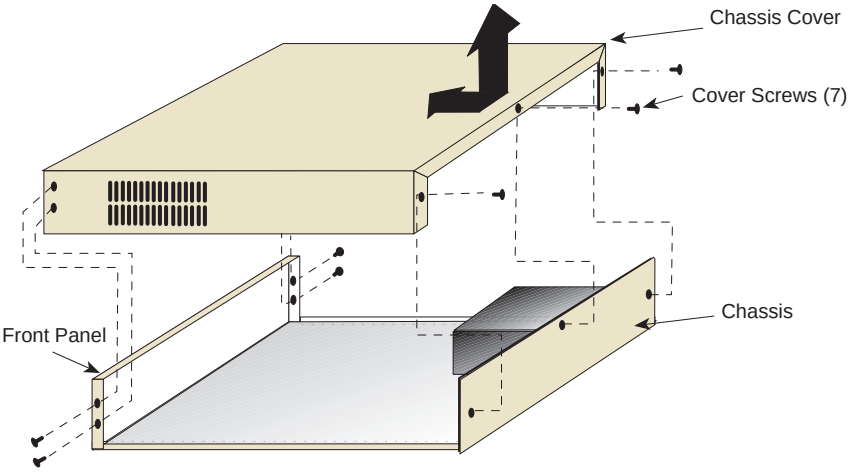
AM HINTEN DES 2H22-08R STECHEI ABZIEHEN UM AUS ZU SCHALTEN.

APAGUE EL 2H22-08R DESENCHUFE EL CABLE DE LA UNIDAD.

Before performing step 1, mark the cables connected to the 2H22-08R according to their associated port numbers. This is recommended for ease of reinstallation.

1. Disconnect all network cables attached to the 2H22-08R.
2. If the 2H22-08R is rack mounted, remove it from the rack and remove the rackmount brackets (refer to Chapter 3).
3. Use a Phillips screwdriver to remove the screws attaching the cover to the chassis. (See Figure C-1.)
4. Remove the cover by sliding it back until it clears the front of the chassis and then lifting it straight up and off the chassis.

To reinstall the chassis cover, perform the removal procedures in reverse.



Note: If the device was rack mounted, the four screws fastening the cover to the front panel are removed and installed along with the rackmount brackets.

2251-30

Figure C-1 Removing the Chassis Cover

C.2.1 Setting the Mode Switch

Figure C-2 shows the location of the mode switches and the switch settings for normal operation. These switches are set at the factory and do not need to be changed.

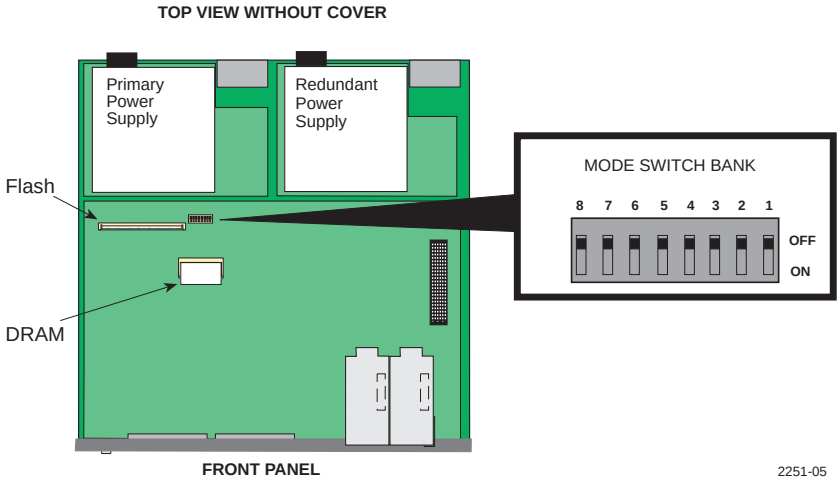
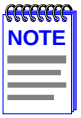


Figure C-2 Mode Switch Location/Component Layout

Switch definitions and positions are as follows:

- **Switches 1 through 4 –** For Cabletron Systems use only.
- **Switch 5 –** COM Port Autobaud. The default (OFF) position enables Autobaud sensing on the COM port for Local Management sessions. Changing the switch to the ON position disables Autobaud sensing and sets the COM port to 9600 baud for Local Management sessions.

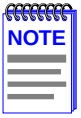
- **Switch 6 –** Forced BootP. The BootP server references the location of a station acting as a Trivial File Transfer Protocol (TFTP) server containing the 2H22-08R image file.



Do NOT attempt a Forced BootP unless a BootP server has been configured for the 2H22-08R.

When the position of Switch 6 is changed and the power is cycled to the 2H22-08R, the device requests the image file location from the BootP server and uses TFTP to download the image from the TFTP server. If one of these requirements is not met, the 2H22-08R will continue to request either the BootP server or the TFTP server until the RESET button on the 2H22-08R is pressed. Once the RESET button is pressed, the 2H22-08R resets after one minute and loads the image stored in FLASH memory.

- **Switch 7 –** Clear NVRAM. Changing the position of this switch resets NVRAM on either the next power-up or the next operation of the front panel RESET button. All user-entered parameters, such as the IP address, device names, etc., are reset to the factory default settings. Once the 2H22-08R resets, you can either use the factory default settings or reenter your own parameters.
- **Switch 8 –** Reset Password/Community Strings. Changing the position of this switch clears user-entered passwords stored in NVRAM, and restores the factory default passwords on either the next power-up or the next operation of the front panel RESET button. Once the 2H22-08R resets, you can either use the factory default settings or reenter your own passwords.



Do not change the position of switch 8 unless it is necessary to reset the 2H22-08R super-user configured passwords to their factory default settings.

C.3 INSTALLING OPTIONAL FAST ETHERNET INTERFACE MODULES

Figure C-3 shows the locations of the Fast Ethernet Interface Module connectors for ports 7 and 8.

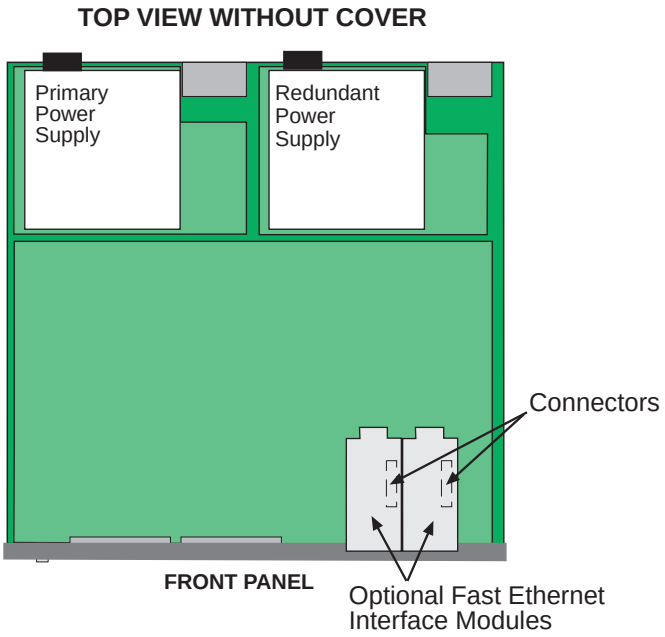


Figure C-3 Fast Ethernet Interface Module Connector Location

To install a Fast Ethernet Interface Module in port slot 7 or 8, proceed as follows:

CAUTION

The FE-100F3 uses Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

CAUTION

The Fast Ethernet Interface Module and the 2H22-08R are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could damage the module or the 2H22-08R.

TIP

When installing Fast Ethernet Interface Modules in both port slots 7 and 8, remove the coverplates from both slot openings. In the following instructions, the optional module is shown being installed in port slot 8.

1. Remove the coverplate from the port slot where the Fast Ethernet Interface Module is to be installed. Refer to Figure C-4 and proceed as follows:

   a. Remove the two screws fastening the coverplate to the standoffs. Save the screws.

   b. Lift and remove the coverplate from the top of the front standoffs.

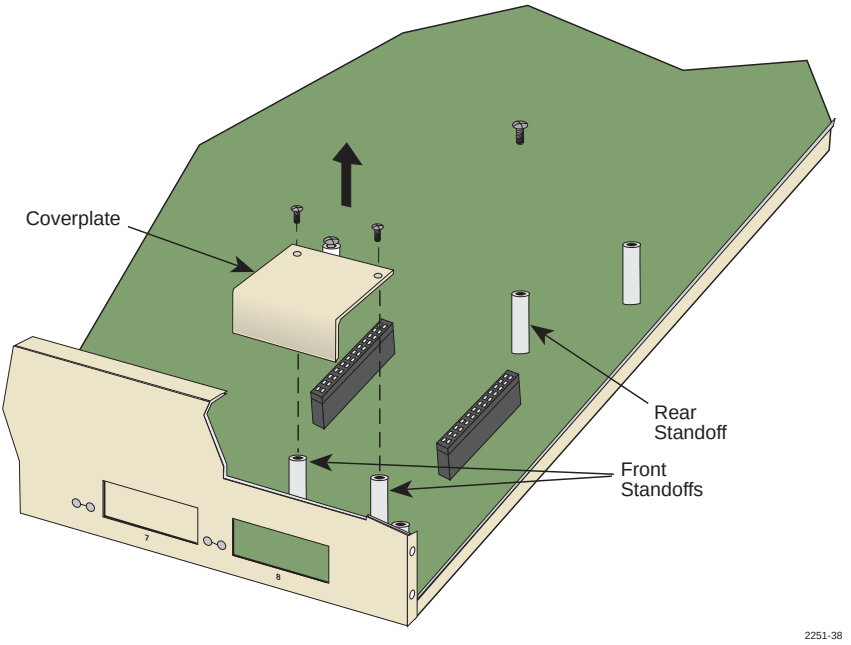


Figure C-4 Coverplate Removal

2. Remove the screw from the rear standoff. Save the screw.

CAUTION

When installing an FE-100FX or FE-100F3 module into the 2H22-08R, remove the rubber plug on the module before proceeding.

3. See Figure C-5. Gently pull the faceplate of the 2H22-08R forward to allow room for the Fast Ethernet Interface Modules to be aligned over the connector.

CAUTION

In the following step, take care when inserting the Fast Ethernet Interface Module into the Motherboard connector, so that the pins do not bend. Otherwise, the Fast Ethernet Interface Board and the Motherboard could be damaged.

4. Carefully lower the Fast Ethernet Interface Module onto the standoffs while inserting the module connector into the associated motherboard connector.

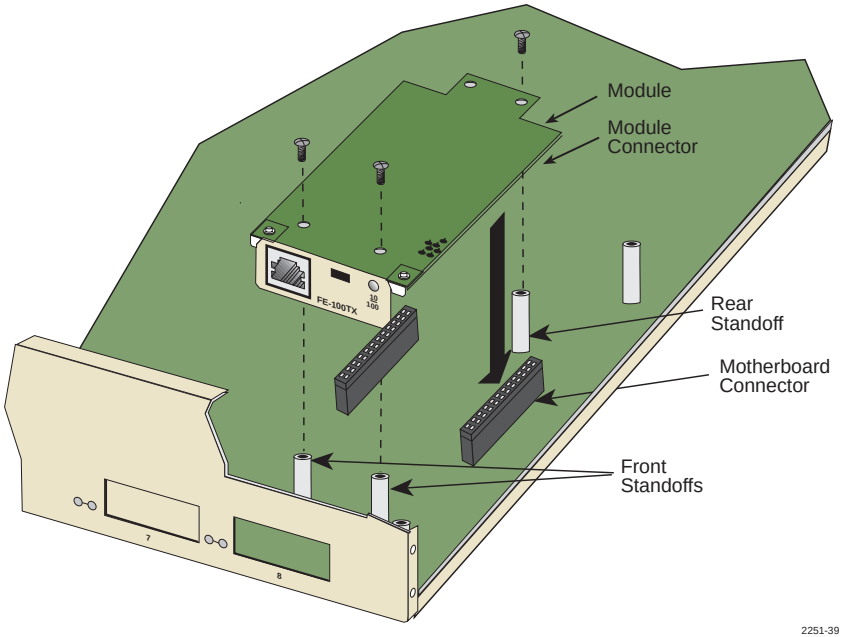


Figure C-5 Installing the Fast Ethernet Interface Module

5. Press down firmly on the Fast Ethernet Interface Module until the pins slide all the way into the motherboard connector. Ensure that the Fast Ethernet Interface Module seats flush on the standoffs.
6. Secure the Fast Ethernet Interface Module with the screws saved in steps 1 and 2.
7. Reinstall the cover.

INDEX