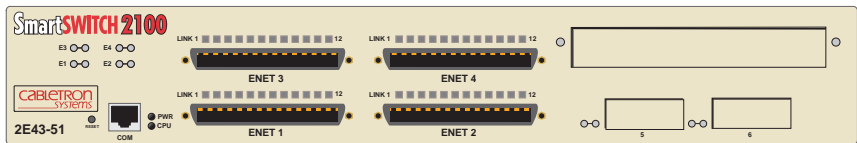


2E43-51/2E43-51R SmartSwitch 2100 User's Guide





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.

© 1998 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005

All Rights Reserved

Printed in the United States of America

Order Number: 9032251-04 September 1998

Cabletron Systems, **LANVIEW**, **QuickSET**, **SecureFast**, and **SPECTRUM** are registered trademarks and **SmartSwitch** is a trademark of Cabletron Systems, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

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.

Printed on



Recycled Paper

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 55×10^{-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 $8 \times 10^3 \text{ W m}^{-2} \text{ sr}^{-1}$.

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

Mr. Ronald Fotino

Full Name

Principal Compliance Engineer

Title

Rochester, NH, USA

Location

Legal Representative in Europe

Mr. J. Solari

Full Name

Managing Director - E.M.E.A.

Title

Newbury, Berkshire, England

Location

CONTENTS

CHAPTER 1 INTRODUCTION

1.1	Using This Guide	1-1
1.2	Structure of This Guide.....	1-1
1.3	2E43-51 Overview	1-3
1.3.1	Connectivity	1-4
1.3.2	Full Duplex Switched Ethernet.....	1-4
1.3.3	Auto-Negotiation	1-4
1.3.4	SmartTrunk	1-5
1.3.5	Runtime IP Address Discovery	1-5
1.3.6	Management	1-6
1.3.7	Switching Options	1-6
1.3.8	Standards Compatibility.....	1-6
1.3.9	Year 2000 Compliant	1-7
1.3.10	LANVIEW Diagnostic LEDs	1-7
1.4	Optional Features	1-7
1.4.1	Fast Ethernet Interface Modules.....	1-7
1.4.2	High Speed Interface Modules	1-8
1.5	Document Conventions	1-8
1.6	Getting Help.....	1-9
1.7	Related Manuals.....	1-10

CHAPTER 2 NETWORK REQUIREMENTS

2.1	SmartTrunk.....	2-1
2.2	10BASE-T Network	2-1
2.3	100BASE-TX Network	2-2
2.4	100BASE-FX Fiber Optic Network	2-2

CHAPTER 3 INSTALLATION

3.1	Required Tools	3-1
3.2	Unpacking the 2E43-51	3-2
3.3	Installing Options	3-2
3.4	Installing the 2E43-51	3-3
3.4.1	Tabletop or Shelf Installation	3-3
3.4.2	Rackmount Installation	3-4
3.4.3	Connecting Power to the Devices.....	3-7
3.4.3.1	Connecting Power to the 2E43-51	3-7
3.4.3.2	Connecting Power to the 2E43-51R.....	3-8

3.5	Connecting to the Network.....	3-9
3.5.1	Connecting Cables to ENETs 1 Through 4	3-9
3.5.2	Connecting a UTP Segment to the FE-100TX	3-11
3.5.3	Connecting a Fiber Optic Segment to the FE-100FX and FE-100F3	3-14
3.6	Completing the Installation.....	3-16

CHAPTER 4 TROUBLESHOOTING

4.1	Using LANVIEW.....	4-1
4.2	FE-100TX LED.....	4-4
4.3	Troubleshooting Checklist.....	4-6
4.4	Using the RESET Button	4-7

CHAPTER 5 LOCAL MANAGEMENT

5.1	Overview	5-1
5.2	Local Management Keyboard Conventions	5-2
5.3	Management Terminal Setup.....	5-3
5.3.1	Console Cable Connection.....	5-4
5.3.2	Management Terminal Setup Parameters	5-5
5.3.3	Telnet Connections	5-6
5.3.4	Monitoring an Uninterruptible Power Supply	5-7
5.4	Accessing Local Management	5-8
5.4.1	Navigating Local Management Screens.....	5-9
5.4.2	Selecting Local Management Menu Screen Items.....	5-11
5.4.3	Exiting Local Management Screens.....	5-11
5.5	Device Menu Screen.....	5-13
5.6	Device Configuration Menu Screen	5-15
5.7	General Configuration Screen	5-17
5.7.1	Setting the IP Address.....	5-20
5.7.2	Setting the Subnet Mask	5-21
5.7.3	Setting the Default Gateway.....	5-22
5.7.4	Setting the TFTP Gateway IP Address	5-23
5.7.5	Setting the Device Date.....	5-24
5.7.6	Setting the Device Time	5-24
5.7.7	Entering a New Screen Refresh Time.....	5-25
5.7.8	Setting the Screen Lockout Time	5-25
5.7.9	Setting the Operational Mode.....	5-26
5.7.10	Configuring the COM Port.....	5-27
5.7.11	Clearing NVRAM	5-29
5.7.12	Enabling/Disabling IP Fragmentation	5-30

5.8	SNMP Community Names Screen	5-31
5.8.1	Establishing Community Names	5-32
5.9	SNMP Traps Screen.....	5-34
5.9.1	Configuring the Trap Table	5-35
5.10	Switch Configuration Screen	5-36
5.10.1	Setting the STA.....	5-38
5.10.2	Setting the Age Time Field	5-38
5.10.3	Setting (Enabling or Disabling) the Port Status	5-39
5.11	Device Specific Configuration Menu Screen	5-39
5.12	System Resources Screen	5-41
5.12.1	Setting the Reset Peak Switch Utilization	5-43
5.13	High Speed Interface Configuration Menu Screen	5-44
5.14	High Speed Interface Configuration Screen	5-46
5.14.1	Configuring an FE-100FX or FE-100F3	5-48
5.14.1.1	Setting the FE-100FX or FE-100F3 Operational Mode	5-49
5.14.2	Configuring an FE-100TX	5-49
5.14.2.1	Setting the FE-100TX Operational Mode	5-49
5.14.2.2	Setting the FE-100TX Advertised Ability	5-50
5.15	FLASH Download Screen.....	5-50
5.15.1	Image File Download Using BootP	5-53
5.15.2	Image File Download Using TFTP	5-53
5.15.3	Image File Download Using Runtime	5-54
5.16	Port Redirect Function Screen	5-55
5.16.1	Displaying the Source and Destination Entries.....	5-57
5.16.2	Changing Source and Destination Ports.....	5-58
5.17	Broadcast Suppression Screen	5-58
5.17.1	Setting the Threshold.....	5-60
5.17.2	Setting the Reset Peak	5-60
5.18	Repeater Configuration Menu Screen	5-61
5.19	Repeater Level Security Configuration	5-62
5.19.1	Setting the Repeater Level Security	5-64
5.20	Port Level Security Configuration Screen.....	5-65
5.20.1	Setting the Port Level Security	5-68
5.21	Device Statistics Menu Screen.....	5-69
5.22	Switch Statistics Screen	5-71
5.23	Interface Statistics Screen.....	5-73
5.23.1	Displaying Interface Statistics	5-76
5.23.2	Using the Clear Counters Command	5-76
5.24	RMON Statistics Screen.....	5-77
5.24.1	Displaying RMON Statistics	5-80
5.24.2	Using the Clear Counters Command	5-81

Contents

5.25	Repeater Statistics Screen	5-81
5.25.1	Displaying Repeater Statistics.....	5-84
5.25.2	Using the Clear Counters Command	5-84
5.26	Network Tools	5-85
5.26.1	Built-in Commands	5-86
5.26.2	Special Commands	5-94

APPENDIX A SPECIFICATIONS

A.1	Device Specifications.....	A-1
A.2	Physical Properties	A-1
A.3	Electrical Specifications	A-1
A.4	Environmental Requirements.....	A-2
A.5	Input/Output Ports.....	A-2
A.6	COM Pinout Assignments.....	A-2
A.7	Regulatory Compliance.....	A-3

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

B.1	FE-100TX.....	B-1
B.2	FE-100FX.....	B-2
B.3	FE-100F3.....	B-3

APPENDIX C OPTIONAL INSTALLATIONS AND MODE SWITCH BANK SETTINGS

C.1	Required Tools.....	C-1
C.2	Removing the Chassis Cover	C-2
C.2.1	Setting the Mode Switch	C-4
C.3	Installing Optional Fast Ethernet Interface Modules	C-7

INDEX

CHAPTER 1

INTRODUCTION

Welcome to the **2E43-51/2E43-51R SmartSwitch 2100 User's Guide**. This guide provides the necessary documentation to install and operate the 2E43-51 and the 2E43-51R SmartSwitch 2100 devices and provides information concerning network requirements, installation, troubleshooting, and the use of Local Management.

1.1 USING THIS GUIDE

Read through this guide to completely understand the 2E43-51 and 2E43-51R 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.



Unless it is noted differently, the information in this guide applies to both the 2E43-51 and the 2E43-51R SmartSwitch 2100 devices. Unless the information pertains only to the 2E43-51 or the 2E43-51R, the device is referred to as either the "2E43-51" or the "device".

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 2E43-51 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 2E43-51.

Chapter 3, Installation, provides instructions on how to install the 2E43-51 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 and use Local Management to configure and manage the 2E43-51.

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 FE-100F3.

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

1.3 2E43-51 OVERVIEW

The 2E43-51 (Figure 1-1) is a repeater/switch device that provides four Ethernet networks (MicroLANs ENET 1 through 4), each consisting of 12 repeater ports that share a bandwidth of 10 Mbps. Each Ethernet network supports 802.1D switching (bridging), and Cabletron Systems SecureFast Switching Virtual Network technology.

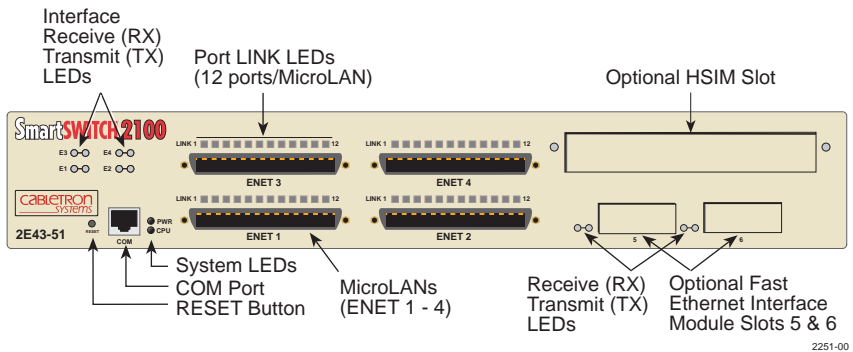


Figure 1-1 The 2E43-51

The 2E43-51 also has two slots (5 and 6) for optional 10/100 Fast Ethernet Interface Modules, and another slot for an optional High Speed Interface Module (HSIM).

The device can switch each Ethernet network (ENET 1 through ENET 4) to one another, to the optional interface modules in slots 5 and 6, and to the HSIM slot. The optional Fast Ethernet Interface Modules provide uplinks to 100BASE-TX or 100BASE-FX Fast Ethernet networks. The HSIMs provide additional connectivity to various networking technologies such as Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI), and Wide Area Network (WAN).

The 2E43-51 may be used as a tabletop unit or can be installed in a standard 19-inch rack using the supplied rack mounting hardware.

The 2E43-51 device has one universal ac power supply with automatic voltage sensing that allows operation using 100–125 or 200–240 Vac, 50/60 Hz.

The 2E43-51R has two power supplies. The power supplies load share 50% (+/-5%) of the power required by the device. If one power supply fails, the remaining power supply assumes the entire load of the device without interruption to network traffic. Each power supply module supports its own ac input connection, which allows the user to connect each power supply to a different ac power circuit.

1.3.1 Connectivity

The 2E43-51 connects to Ethernet networks or workstations through four 50-pin RJ21 connectors. Each connector serves as a 12-port Ethernet 10 Mbps MicroLAN.

Both of the devices have two front panel slots (ports 5 and 6) for optional Fast Ethernet Interface Modules to support an uplink to 100 Mbps Fast Ethernet backbones or a high speed connection to a local server. There is also space for an optional HSIM to provide additional connectivity to various networking technologies.

1.3.2 Full Duplex Switched Ethernet

The optional Fast Ethernet Interface Modules for the 2E43-51 can be configured to operate in Full Duplex Switched Ethernet mode, which provides 200 Mbps of bandwidth.

1.3.3 Auto-Negotiation

The repeater ports and Fast Ethernet Interface Modules can auto-negotiate the type of connection required to provide a link to another device. During Auto-Negotiation, two devices automatically exchange information “telling” each other what their operating capabilities are. The Auto-Negotiation feature targets the maximum capabilities that can be reached between the two devices. For example, an FE-100TX Fast Ethernet Interface Module in a 2E43-51 can adjust to 100 Mbps when the device on the other end of the connection can also adjust to 100 Mbps. If the device on the other end of the connection can only operate at 10 Mbps, then the FE-100TX simply 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 FE-100TX cannot auto-negotiate, the FE-100TX Fast Ethernet Interface Module operates according to the capabilities of the other device.

1.3.4 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.

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

1.3.5 Runtime IP Address Discovery

This feature enables the 2E43-51 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 2E43-51 is connected to the network and powered up, Runtime IP Address Discovery (RAD) checks the 2E43-51 for an IP address. If one has not yet been assigned (2E43-51 IP address set to 0.0.0.0), RAD checks to see if any of the 2E43-51 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.

1.3.6 Management

Management of the 2E43-51 is accomplished using SNMP compliant management tools for in-band Local Management. Out-of-band Local Management is provided through the RJ45 COM port on the front panel using a VT100 terminal or a VT100 terminal emulator. In-band remote management is possible through any SNMP compliant Network Management Software.

Local Management provides the ability to manage the 2E43-51 and any of the optional Fast Ethernet Interface Modules installed in ports 5 and 6, and the optional High Speed Interface Module (HSIM).

The associated HSIM user's guide provides detailed information about the HSIM Local Management.

1.3.7 Switching Options

The 2E43-51 provides 802.1D switching, 802.1Q switching or SecureFast Switching Virtual Network Services between all of the front panel interfaces including Fast Ethernet Interface Modules and High Speed Interface Module (HSIM).

IEEE 802.1Q switching and SecureFast switching allow for future migration to Virtual Network technologies without requiring the replacement of existing equipment.

1.3.8 Standards Compatibility

The 2E43-51 provides IEEE 802.1D Spanning Tree Algorithm (STA) support to enhance the overall reliability of the network and protect against "loop" conditions. The 2E43-51 also supports 100BASE-TX and 100BASE-FX Fast Ethernet standards and 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 provide a wide array of statistical information to enhance troubleshooting.

1.3.9 Year 2000 Compliant

The 2E43-51 has an internal clock that can maintain the current time and date beyond the year 1999.

1.3.10 LANVIEW Diagnostic LEDs

LANVIEW diagnostic LEDs serve as an important troubleshooting aid by providing an easy way to observe the status of individual ports and overall network operations.

1.4 OPTIONAL FEATURES

Options for the 2E43-51 include the following:

- Fast Ethernet Interface Modules
- High Speed Interface Modules

1.4.1 Fast Ethernet Interface Modules

Cabletron Systems provides Fast Ethernet Interface Modules to support uplinks to 100 Mbps Fast 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

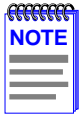
P/N	Description	Application
FE-100TX	Uses RJ45 connector	Supports Category 5 Unshielded Twisted Pair (UTP) cabling, which has an impedance of 85 to 111 ohms, and Shielded Twisted Pair (STP) cabling.
FE-100FX	Uses SC connector	Supports multimode fiber optic cabling.
FE-100F3	Uses SC connector	Supports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

1.4.2 High Speed Interface Modules

High Speed Interface Modules (HSIMs) are available from Cabletron Systems for additional connectivity to various networking technologies. The HSIMs available for the 2E43-51 are listed in the Release Notes shipped with the 2E43-51.

1.5 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.



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



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

1.6 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	ftp://ftp.cabletron.com/
Login	<i>anonymous</i>
Password	<i>your email address</i>
<p>To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: TechWriting@cabletron.com <i>Make sure to include the document Part Number in the email message.</i></p>	

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

1.7 RELATED MANUALS

The following manuals may help to set up, control, and manage the 2E43-51:

Cabletron Systems *HSIM-A6DP User's Guide*

Cabletron Systems *HSIM-F6 User's Guide*

Cabletron Systems *HSIM-FE6 User's Guide*

Cabletron Systems *HSIM-W87 User's Guide*

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

Cabletron Systems *Ethernet Technology Guide*

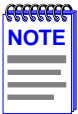
Cabletron Systems *Cabling Guide*

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.

Documents for the Cabletron Systems HSIM-W6 and HSIM-W84 devices are contained on the QuickSET CD-ROM and are also available on the World Wide Web at: <http://www.cabletron.com/>.

CHAPTER 2

NETWORK REQUIREMENTS

This chapter contains networking guidelines. Before installing and using the 2E43-51 or an optional Fast Ethernet Interface Module (FE-100TX, FE-100FX, or FE-100F3), review the requirements and specifications outlined in this chapter concerning the following:

- SmartTrunk (Section 2.1)
- 10BASE-T Twisted Pair Network (Section 2.2)
- 100BASE-TX Twisted Pair Network (Section 2.3)
- 100BASE-FX Fiber Optic Network (Section 2.4)

The network installation must meet the guidelines to ensure satisfactory performance of this equipment. Failure to follow the guidelines may produce poor network performance.



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

2.1 SmartTrunk

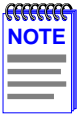
To connect the 2E43-51 into a network so that it can take advantage of the SmartTrunk feature, there are certain rules concerning port connections and configurations that must be followed for proper operation. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

2.2 10BASE-T NETWORK

When connecting a 10BASE-T segment to any of the 2E43-51 ports (ENET 1 through ENET 4), ensure that the network meets IEEE 802.3 Ethernet network requirements for 10BASE-T. Refer to the Cabletron Systems *Cabling Guide* for details.

2.3 100BASE-TX NETWORK

The 2E43-51, with an FE-100TX installed in slots 5 and/or 6, provides an RJ45 connection that supports UTP cabling, which has an impedance of 85 to 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 2E43-51 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 adjust its speed accordingly.

2.4 100BASE-FX FIBER OPTIC NETWORK

Slots 5 and 6 of the 2E43-51 can also 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 Mode 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 length of a 100BASE-FX segment may be no more than 412 meters between Data Terminal Equipment (DTE to DTE) in half duplex mode or 20 km (DTE to DTE) in full duplex mode.

CHAPTER 3

INSTALLATION



Only qualified personnel should install the 2E43-51.

This chapter provides the instructions required to install the 2E43-51. Follow the order of the sections listed below to correctly install the 2E43-51.

- Required Tools ([Section 3.1](#))
- Unpacking the 2E43-51 ([Section 3.2](#))
- Installing Options ([Section 3.3](#))
- Installing the 2E43-51 (on a shelf or tabletop, or into a standard rack) ([Section 3.4](#))
- Connecting to the Network ([Section 3.5](#))
- Completing the Installation ([Section 3.6](#))

3.1 REQUIRED TOOLS

A Phillips screwdriver is required to install the 2E43-51 in a rack.

3.2 UNPACKING THE 2E43-51

To unpack the 2E43-51 and verify the contents of the shipment, proceed as follows:

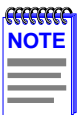
1. Open the carton and remove the packing material protecting the 2E43-51.
2. Verify the contents of the carton as listed in [Table 3-1](#).

Table 3-1 Contents of 2E43-51 Carton

Item	Quantity
2E43-51	1
Antistatic wrist strap	1
Console Cable Kit	1
RJ21 Angle Adapter	4
Rackmount Kit	1
Strain Relief Bracket	1
Release Notes	1
Power Cord (2E43-51 only)	1
Power Cord (2E43-51R only)	2

3. Remove the black and yellow tape seal on the non-conductive bag to remove the 2E43-51.
4. Perform a visual inspection of the device for any signs of physical damage. If there are any items missing or damaged, contact the Cabletron Systems Global Call Center as described in [Section 1.6](#).

3.3 INSTALLING OPTIONS



Install any optional equipment before proceeding to [Section 3.4](#).

If the 2E43-51 is to be installed with an optional Fast Ethernet Interface Module, refer to [Appendix C](#) for installation instructions. The installation instructions for the HSIMs are in the associated HSIM user's guide.

3.4 INSTALLING THE 2E43-51

The 2E43-51 may be installed on a tabletop, shelf, or in a 19-inch rack. [Section 3.4.1](#) describes a tabletop or shelf installation, and [Section 3.4.2](#) describes the rackmount installation.



To prevent possible personal injury and/or damage to the unit, do **NOT** connect power to the 2E43-51 until instructed to do so.

3.4.1 Tabletop or Shelf Installation

The following two subsections provide guidelines for installation on a tabletop or shelf.

Guidelines for Tabletop and Shelf Installations

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

- Locate the 2E43-51 within seven feet of an appropriately grounded power receptacle 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 2E43-51.
- 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.
- Maintain a 2-inch clearance from the left, right, and rear sides of the device to provide adequate ventilation.

Installation

For a tabletop or shelf installation, locate the 2E43-51 within seven feet of its power source and with an unrestricted free surface area as shown in [Figure 3-1](#). Proceed to [Section 3.4.3](#) for power connection instructions.



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 2E43-51.

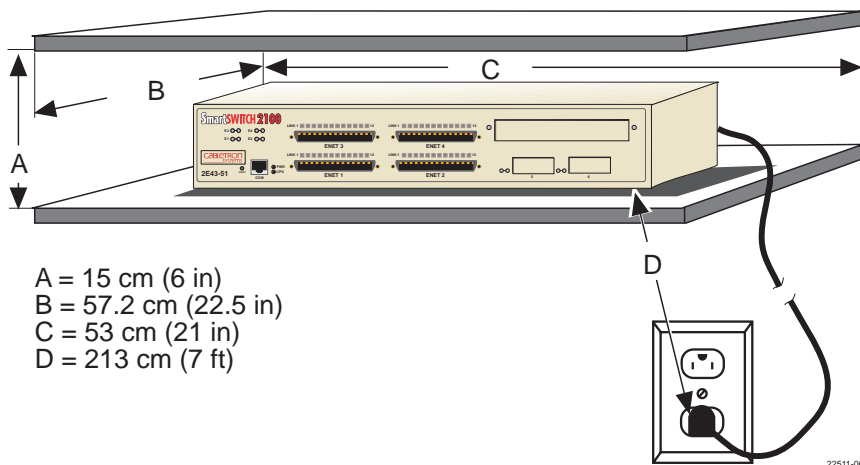


Figure 3-1 Tabletop or Shelf Installation

3.4.2 Rackmount Installation

To install the 2E43-51 in a 19-inch rack, the device is shipped with a rackmount kit containing the rackmount brackets, mounting screws, and a strain-relief bracket for cable management.

Guidelines for the Rackmount Installation

The installation site must be within reach of the network cabling and meet the requirements listed below:

- An appropriate grounded power receptacle must be located within seven feet of the location.
- 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.



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 2E43-51.



Before installing the 2E43-51 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.

Installation

Rack mounting the 2E43-51 involves the following:

- Attaching the strain-relief bracket
- Rack mounting the 2E43-51 (attaching the mounting brackets and fastening the 2E43-51 to the rack)

Attaching the Strain-Relief Bracket

Attach the strain-relief bracket to the front of the 2E43-51 as follows:

1. Locate the strain-relief bracket and four 8-32 x 5/16-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 5/16-inch screws included with the 2E43-51. Use of longer screws may damage the unit.

2. Attach the strain-relief bracket to the bottom of the 2E43-51 using the four 8-32 x 5/16-inch pan-head screws (Figure 3-2).

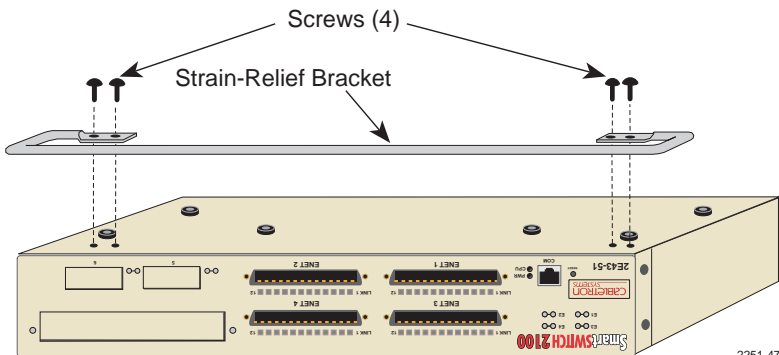
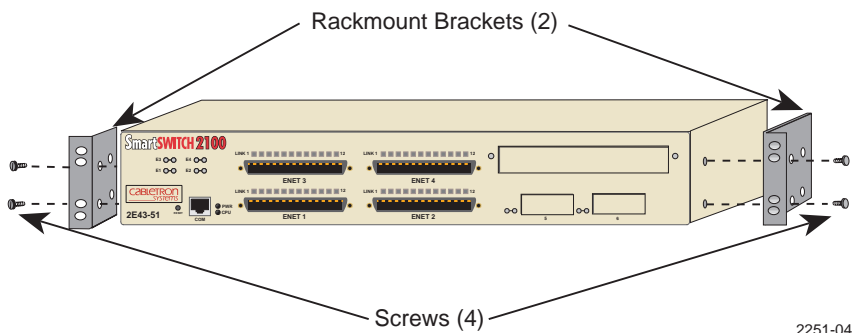


Figure 3-2 Attaching the Strain-Relief Bracket

Rack Mounting the 2E43-51

Proceed as follows to install the 2E43-51 into a 19-inch rack.

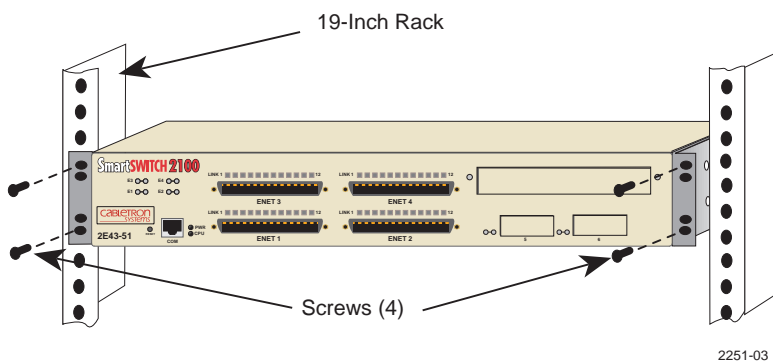
1. Remove and discard the four cover screws (two from each side) located along the front edges of each side of the 2E43-51.
2. Locate the four 6-32 x 3/8-inch flathead cover replacement screws in the rackmount kit. Use these screws to attach the rackmount brackets to the 2E43-51 as shown in [Figure 3-3](#).



2251-04

Figure 3-3 Installing the Rackmount Brackets

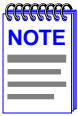
3. With the mounting brackets installed, position the 2E43-51 between the vertical frame members of the 19-inch rack and fasten it securely with user supplied mounting screws as shown in [Figure 3-4](#).



2251-03

Figure 3-4 Installing the 2E43-51 in a Rack

3.4.3 Connecting Power to the Devices



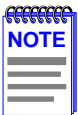
The 2E43-51 has one power supply while the 2E43-51R has two. The power supplies have automatic voltage sensing that allows connection to power sources ranging from 100–125 Vac, 2.0 A or 200–240 Vac, 1.0 A, 50/60 Hz.

To connect power to the 2E43-51, proceed to [Section 3.4.3.1](#). To connect power to the 2E43-51R, proceed to [Section 3.4.3.2](#).

3.4.3.1 Connecting Power to the 2E43-51

To connect the 2E43-51 to a power source, proceed as follows:

1. Plug the power cord into a grounded wall outlet. The PWR LED turns on (green) and the CPU LED turns on (green) briefly.



It takes approximately one minute for the 2E43-51 to boot up.

2. Observe the LANVIEW LEDs. After a successful boot, the CPU LED turns on (green). If the CPU LED is not green after one minute, check the power cord connection and power source. If the CPU LED is still not green, contact the Cabletron Systems Global Call Center. Refer to [Section 1.6](#) for details.

3.4.3.2 Connecting Power to the 2E43-51R

To connect the 2E43-51R to the power sources, proceed as follows:

1. Plug each power cord 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.

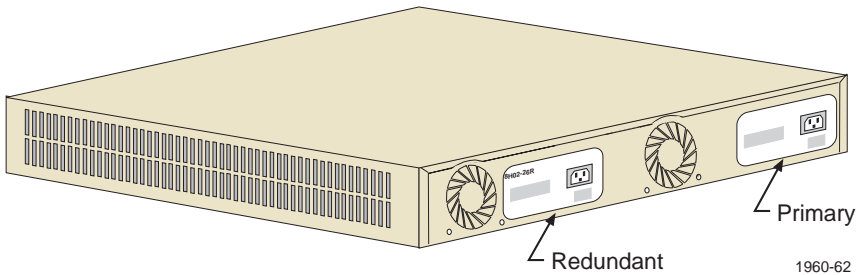
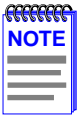


Figure 3-5 2E43-51R Rear View

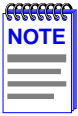


It takes approximately one minute for the 2E43-51R to boot up.

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 1.6](#) for details.

3.5 CONNECTING TO THE NETWORK

This section provides the procedures for connecting UTP and fiber optic segments from the network or other devices to the 2E43-51.



If the 2E43-51 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 *SmartTrunk User's Guide* for the configuration information.

Ports 1 through 4 are MicroLANs (ENET 1 through 4) with each one consisting of 12 UTP connections via a 50-pin RJ21 connector. Ports 5 and 6 support FE-100TX, FE-100FX, or FE-100F3 Fast Ethernet Interface Modules.

The FE-100TX has an RJ45 connector for a UTP cable connection. The FE-100FX and FE-100F3 have SC connectors for fiber optic cable connections.

Refer to [Section 3.5.1](#) to make UTP connections to ENET 1 through ENET 4.

Refer to [Section 3.5.2](#) to make a UTP connection to an FE-100TX in port slot 5 or 6.

Refer to [Section 3.5.3](#) to make a fiber optic cable connection to an FE-100FX or FE-100F3 in port slot 5 or 6.

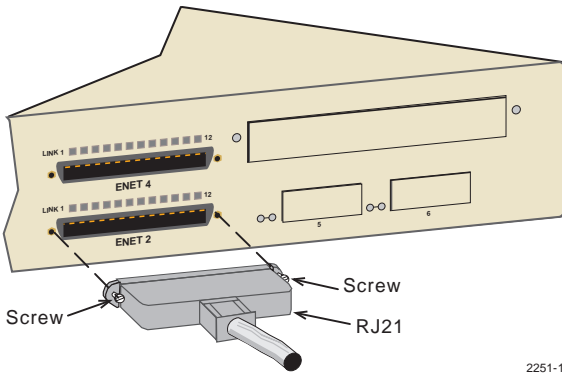
Refer to the associated High Speed Interface Module user's guide to make connections to an optional High Speed Interface Module installed in the HSIM slot.

3.5.1 Connecting Cables to ENETs 1 Through 4

The device uses four RJ21 connectors for the MicroLAN (ENET) connections, each supporting 12 Ethernet ports. All Ethernet ports have internal crossovers.

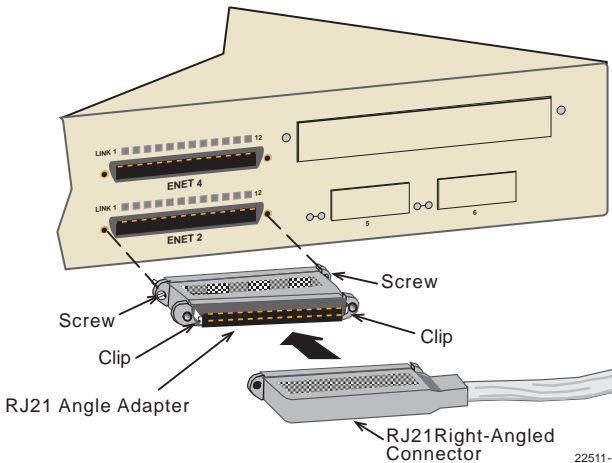
To connect an RJ21, proceed as follows:

1. Ensure that the device connected to the other end of the segment is powered on.
2. If using an RJ21 straight connector, plug it into the appropriate RJ21 port as shown in **Figure 3-6** or, if using the RJ21 angle adapter supplied with the device, insert the RJ21 angle adapter as shown in **Figure 3-7**. The RJ21 angle adapter allows the cables to be dressed along the front of the device and easily attached to the strain-relief bracket when using a right-angled RJ21 connector.



2251-10

Figure 3-6 Straight Cable Connection



22511-73

Figure 3-7 Connection Using the RJ21 Angle Adapter

3. Tighten the two screws on the RJ21 straight cable connector or RJ21 angle adapter, as applicable, to secure it to the device.



The cable pinouts for a 25 pair cable (RJ21) can be found in the Cabletron Systems *Cabling Guide*. Refer to [Section 1.7](#) for details on how to obtain this document.

4. If using the RJ21 angle adapter, plug in the RJ21 right-angled connector until the two retaining clips, shown in [Figure 3-7](#), snap into place.
5. Verify that a link exists by checking that the **LINK LED** on the 2E43-51 for that port is on (solid green). If the **LINK LED** is off, perform the following steps until it is on:
 - a. Verify that the 10BASE-T device at the other end of the twisted pair segment is on and connected to the segment.
 - b. Verify that all connectors on the twisted pair segment have the proper pinouts and check the cable for continuity.
 - c. Check that the twisted pair connection meets the dB loss and cable specifications outlined in [Chapter 2](#).

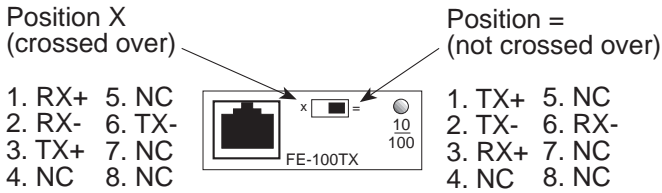
If a link is not established, contact Cabletron Systems Global Call Center. Refer to [Section 1.6](#) for details.

6. Repeat steps 1 through 4 above, until all connections have been made.

3.5.2 Connecting a UTP Segment to the FE-100TX

The FE-100TX supports Category 5 UTP cabling, which has an impedance of 85 to 11 ohms.

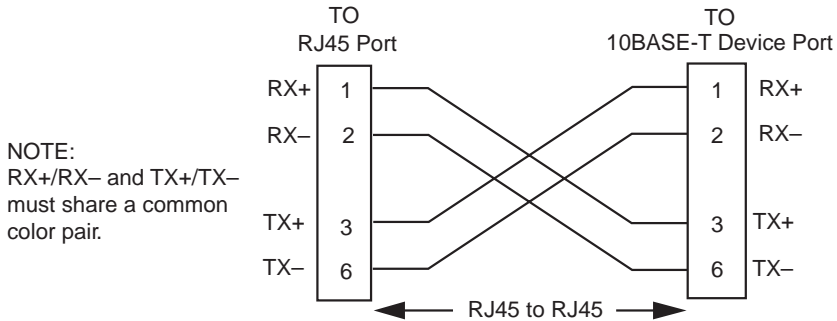
An FE-100TX installed in port slot 5 and/or 6 has an internal crossover switch. When connecting a workstation, use a straight-through cable and set the Fast Ethernet Interface Module crossover switch shown in [Figure 3-8](#) to the crossed over position marked with X. When connecting networking devices, such as another bridge, repeater, or router, use a straight-through cable and set the Fast Ethernet Interface Module crossover switch shown in [Figure 3-8](#) to the straight-through position (not crossed over), marked with =.



16651_05

Figure 3-8 FE-100TX Crossover Switch

A schematic of a crossover cable is shown in Figure 3-9. If the wires do not cross over, use the switch on the FE-100TX to internally cross over the RJ45 port.



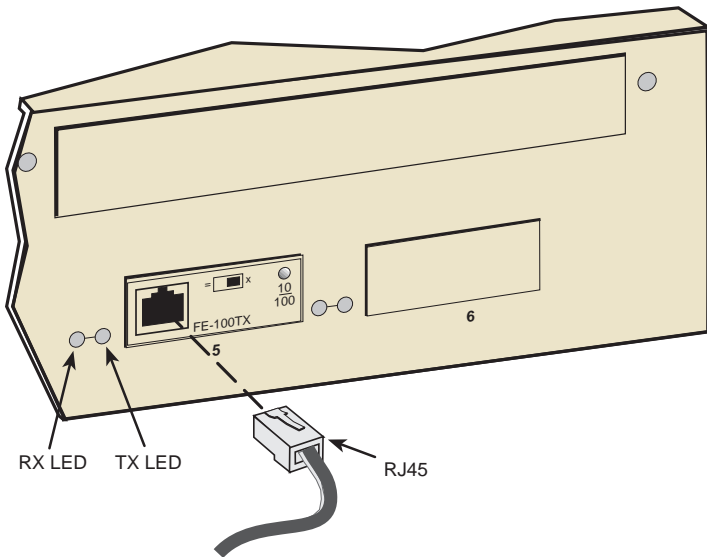
NOTE:
RX+/RX- and TX+/TX- must share a common color pair.

2251-31

Figure 3-9 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 to the module by inserting the RJ45 connector on the twisted pair segment into the RJ45 port on the module shown in Figure 3-10.



2251-14

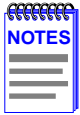
Figure 3-10 FE100-TX Port

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 [Section 2.3](#).
 - e. Confirm that the crossover switch is in the correct position.

If a Link is not established, contact the Cabletron Systems the Global Call Center. Refer to [Section 1.6](#) for details.

3.5.3 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 3-11](#). 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.



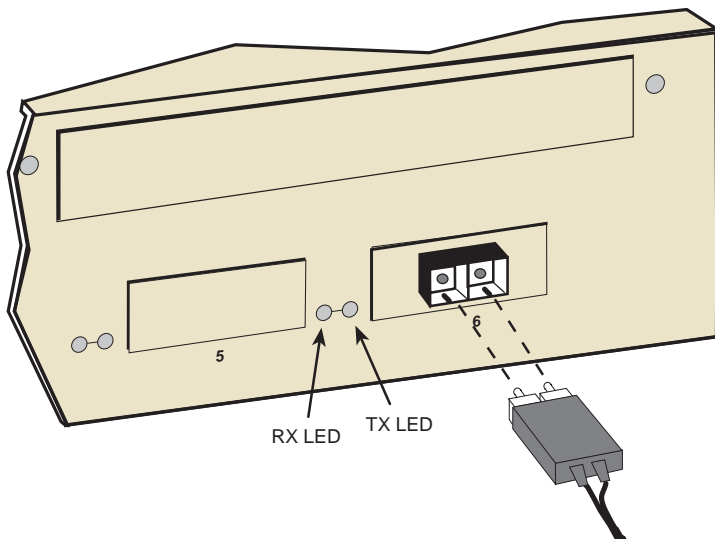
The FE-100F3 uses Class 1 lasers. Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.



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, blow the surfaces with a canned duster. A fiber port cleaning swap saturated with optical-grade isopropyl alcohol may also be used to clean the fiber optic ends.

2. Insert one end of the SC connector into the FE-100FX or FE-100F3 installed in the 2E43-51. See [Figure 3-11](#).

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



2251-34

Figure 3-11 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). 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 2E43-51 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 1.6](#) for details.

3.6 COMPLETING THE INSTALLATION

After installing the 2E43-51 and any optional Fast Ethernet Interface Modules and HSIM as appropriate, 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 2E43-51 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 2E43-51.

CHAPTER 4

TROUBLESHOOTING

This chapter provides information concerning the following:

- Using the LANVIEW diagnostic and status monitoring system
- Troubleshooting network and 2E43-51 operational problems
- Using the RESET button

4.1 USING LANVIEW

The 2E43-51 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 diagnosing 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.

All LEDs for the High Speed Interface Module (HSIM) are located on the HSIM and are described in the associated HSIM user's guide.

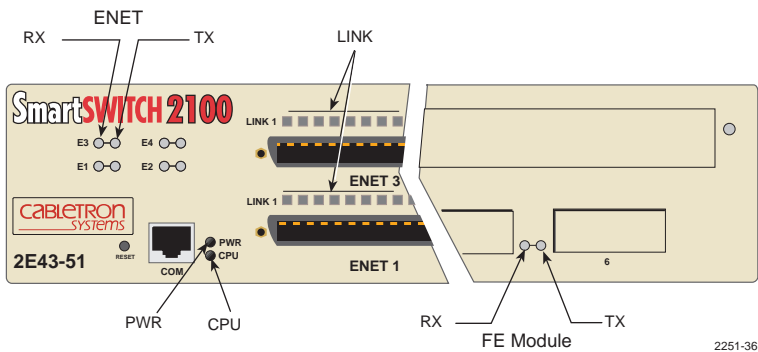
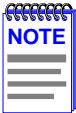


Figure 4-1 LANVIEW LEDs



The terms **flashing**, **blinking**, and **solid** used in the following tables indicate the following:

Flashing indicates an LED pulse that is not flashing at a random rate.

Blinking indicates an LED pulse flashing at a steady rate (50% on, 50% off).

Solid indicates a steady LED light. No pulsing.

Table 4-1 LANVIEW LEDs

LED	Color	State	Recommended Action
PWR	Green	Functional. Power supply(ies) operating normally.	No action.
	Amber	This indication only applies when there are two power supplies. Indicates loss of power supply redundancy.	1. Ensure that the power cords are plugged in correctly and that there is power at the power source. 2. Contact the Cabletron Systems Global Call Center.
CPU	Off	Power off.	Power up device.
	Red	Blinking. Hardware failure has occurred.	Contact the Cabletron Systems Global Call Center.
		Solid. Resetting, normal power up reset.	No action.
	Amber	Blinking. Crippled.	Contact the 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.	

Table 4-1 LANVIEW LEDs (Continued)

LED	Color	State	Recommended Action
RX (Receive) of ENET 1 – 4 and Ports 5 and 6	Off	No link. No activity. Port enabled or disabled.	No error.
	Green	Blinking. Port disabled.	No error.
	Amber	Flashing. Port enabled, activity.	No error.
	Red	Diagnostic failure.	Contact the Cabletron Systems Global Call Center for assistance.
TX (Transmit) LED of ENET 1 – 4 and Ports 5 and 6	Off	Port enabled, and no activity. Should flash green every two seconds indicating BPDUs being sent if STA is enabled and there is a valid link.	<ol style="list-style-type: none"> 1. Ensure that the STA is enabled and that there is a valid link. 2. Contact the Cabletron Systems Global Call Center for assistance.
	Green	Flashing. Indicates activity. Rate indicates data rate.	No action.
	Amber	Blinking. Port in standby. Port may be disabled due to Spanning Tree.	<ol style="list-style-type: none"> 1. Ensure that the port is not disabled. 2. Contact the Cabletron Systems Global Call Center for assistance.
	Red	Flashing. Indicates collision rate.	No action.
Solid. Diagnostic failure.		Contact the Cabletron Systems Global Call Center for assistance.	
LINK Ports of ENET 1 – 4	Amber	Solid. A link is established with the device connected to the port.	No action.
		Flashing. Link established, but administratively disabled.	No action.
		Off. No link.	No action.

4.2 FE-100TX LED

The optional FE-100TX has one LED labeled 10/100. The 10/100 LED together with the RX 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. Tables 4-2 and 4-3 provide a functional description of the 10/100 LED when the RX LED is on or off, respectively.

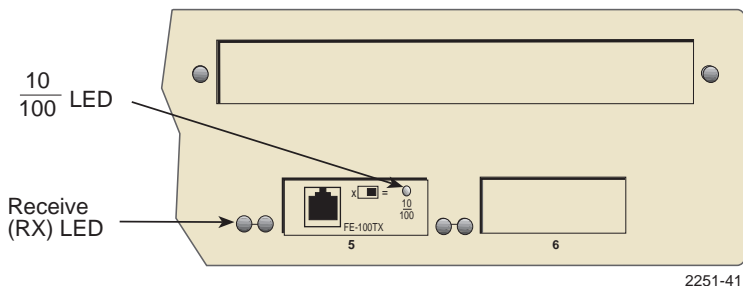
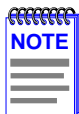


Figure 4-2 FE-100TX LED



A link exists if the associated port (5 or 6) RX LED is on.

Table 4-2 10/100 LED Indications When RX LED Is On

LED	Color	Indication
10/100	Off	FE-100TX is operating at 10 Mbps.
	Green	FE-100TX is operating at 100 Mbps.



No link exists if the associated port (5 or 6) RX LED is off.

Table 4-3 10/100 LED Indications When RX LED Is Off

LED	Color	Indication
10/100	Off	No Link or no cable attached. FE-100TX forced to 10 Mbps operation, or is manually set to "auto-negotiate" mode.
	Green	No Link or no cable attached. FE-100TX is forced to 100 Mbps operation.

4.3 TROUBLESHOOTING CHECKLIST

If the 2E43-51 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.	Check for proper connection of the power cable and its access to a live outlet.
	Installed improperly.	Check the installation.
No Local Management Password screen.	Autobaud is 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 used.	Refer to Appendix A for proper console port pinouts.
Cannot contact the 2E43-51 from in-band management.	Using incorrect Community Name.	Refer to Chapter 5 for Community Name setup.
	The 2E43-51 does not have an IP address assigned.	Refer to Chapter 5 for IP address assignment procedure.
	Port is disabled.	Enable port.
	No link to device.	Check link to device.
Port(s) goes into standby for no apparent reason.	The 2E43-51 detected a loop condition.	<ol style="list-style-type: none"> 1. Review network design and delete unnecessary loops. 2. Call the Cabletron Systems Global Call Center if the problem continues.
User parameters (IP address, Device and Module name, etc.) were lost when the 2E43-51 power was cycled or the front panel RESET button was 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.	<ol style="list-style-type: none"> 1. Reenter the lost parameters as necessary. 2. Call the Cabletron Systems Global Call Center if the problem continues.

4.4 USING THE RESET BUTTON

The RESET button shown in Figure 4-3 resets the 2E43-51 processor without affecting the NVRAM.



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.

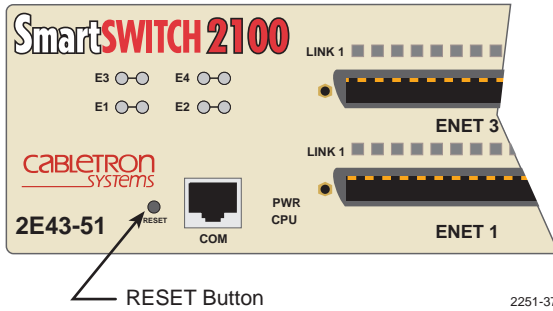


Figure 4-3 RESET Button

To reset the 2E43-51 processor, press and release the RESET button. The 2E43-51 goes through a reset process for approximately 45 seconds.

CHAPTER 5

LOCAL MANAGEMENT

This chapter explains how to set up a management terminal to access Local Management. It also explains how to use the Local Management screens and commands.

5.1 OVERVIEW

Local Management for the 2E43-51 consists of a series of screens that allow the management of the 2E43-51 and its attached segments. The screens allow the user to do the following tasks:

- Assign IP address and subnet mask
- Select a default gateway
- Control access by establishing community names
- Download a new operation software image
- Designate which Network Management Workstations receive SNMP traps from the device
- View statistics
- Configure ports
- Control the number of receive broadcasts that are switched out to the other interfaces
- Clear NVRAM

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port
- 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 appear 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 allows 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 2E43-51 to attach the management terminal to the 2E43-51 COM port as shown in Figure 5-1.

Connect an IBM PC or compatible device, running the VT terminal emulation, to the 2E43-51 as follows:

1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the 2E43-51.
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.

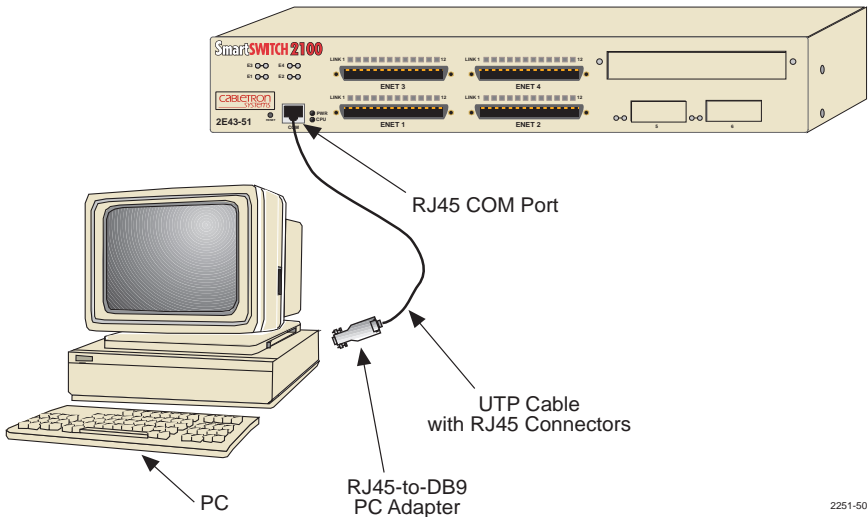


Figure 5-1 Management Terminal Connection

2251-60

5.3.2 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

5.3.3 Telnet Connections

Once the 2E43-51 has a valid IP address, the user can establish a Telnet session with Local Management from any TCP/IP based node on the network. Telnet connections to the 2E43-51 require the community name passwords assigned at the SNMP Community Names screen of the 2E43-51.

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.

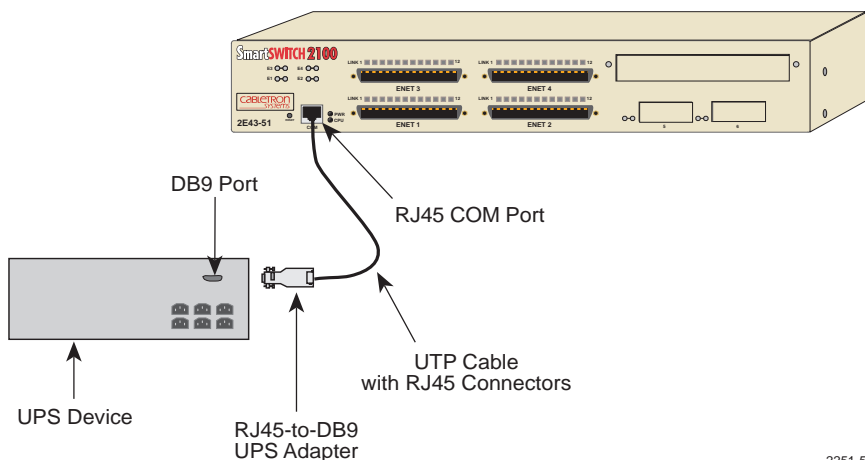
5.3.4 Monitoring an Uninterruptible Power Supply

If the 2E43-51 is connected to an Uninterruptible Power Supply (UPS) device for protection against the loss of power, a connection from the 2E43-51 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.

The Console Cable Kit provided with the 2E43-51 is used to attach the UPS to the 2E43-51 COM port as shown in [Figure 5-2](#).

To connect the UPS device to the COM port of the 2E43-51, proceed as follows:

1. Connect the RJ45 connector at one end of the cable to the COM port on the 2E43-51.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 male (UPS) adapter.
3. Connect the RJ45-to-DB9 male (UPS) adapter to the female DB9 port on the rear of the UPS device (see the particular UPS device's user instructions for more specific information about the monitoring connection).



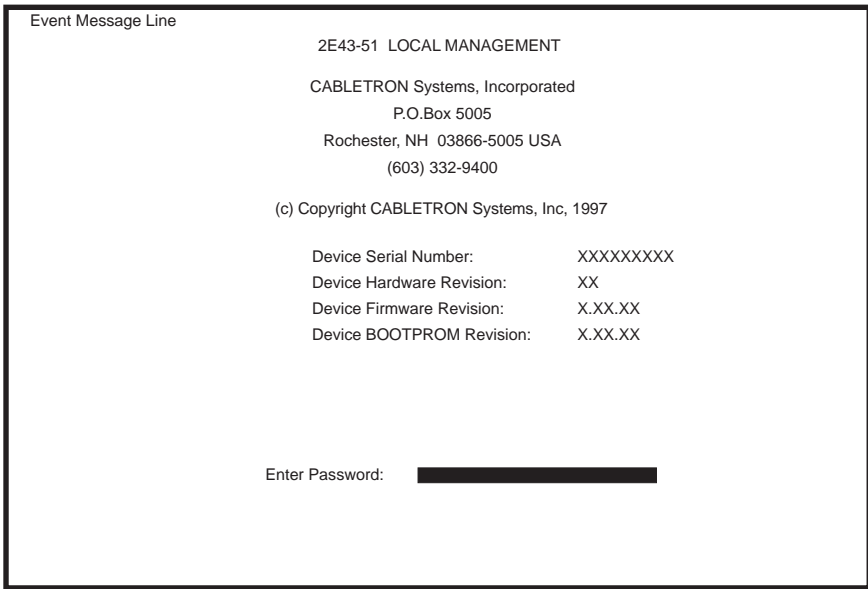
2251-51

Figure 5-2 Uninterruptible Power Supply (UPS) Connection

5.4 ACCESSING LOCAL MANAGEMENT

Access to Local Management is controlled through the Local Management Password screen [Figure 5-3](#). Whenever a connection is made to the 2E43-51 the Local Management Password screen displays. Before continuing, the user must enter a password (community name) which is compared to the previously stored passwords. The level of access allowed the user depends on the password. To set or change passwords, refer to [Section 5.8](#). The following steps describe the procedure to access Local Management.

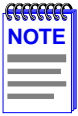
1. Turn on the terminal. Press ENTER (up to four times) until the 2E43-51 Local Management Password screen displays. It is the automatic line speed seeking feature of the port that makes it necessary at times to press ENTER several times.



22511-12

Figure 5-3 The 2E43-51 Local Management Password Screen

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



The 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.

Entering a valid password causes the associated access level to display at the bottom of the screen and the Device Menu screen to appear.

If no activity occurs for several minutes, the Local Management Password screen redisplay and the password has to be reentered.

5.4.1 Navigating Local Management Screens

The 2E4X-27 Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens.

The 2E43-51 supports three modes of switch operation. The switching modes are as follows:

- 802.1D Switching (traditional switching)
- 802.1Q Switching (port based VLAN switching)
- SecureFast VLAN (Cabletron Systems SecureFast switching)

Depending on the Operational Mode set for the device, the hierarchy of the 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.

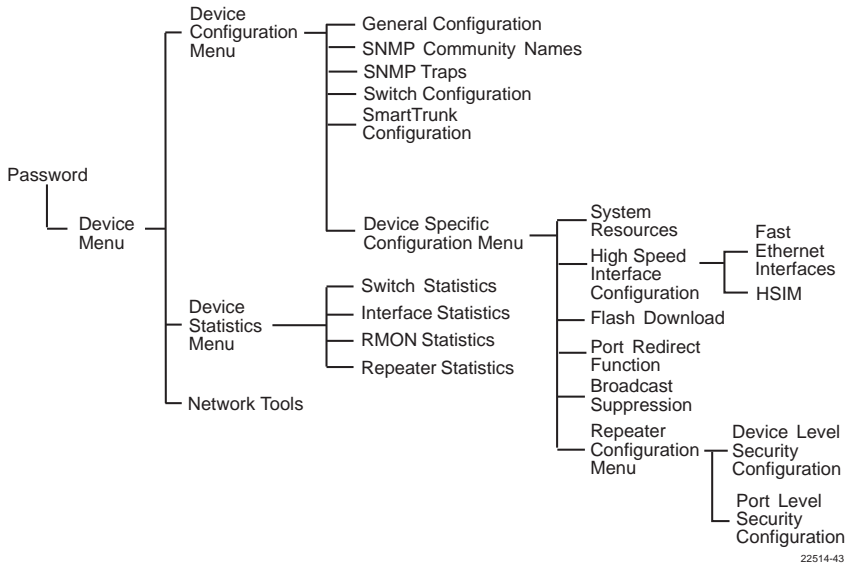


Figure 5-4 802.1D Switching Mode, LM Screen Hierarchy

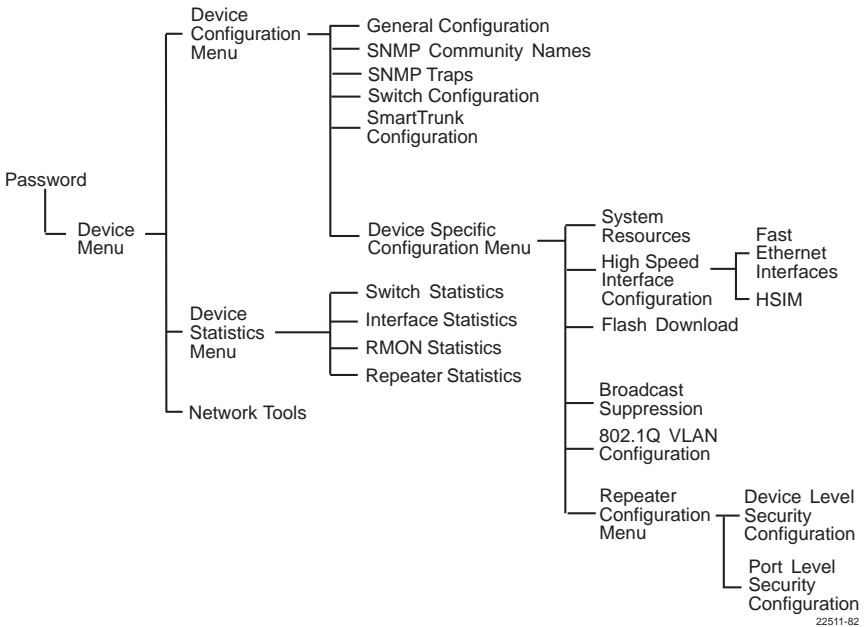


Figure 5-5 802.1Q Switching Mode, LM Screen Hierarchy

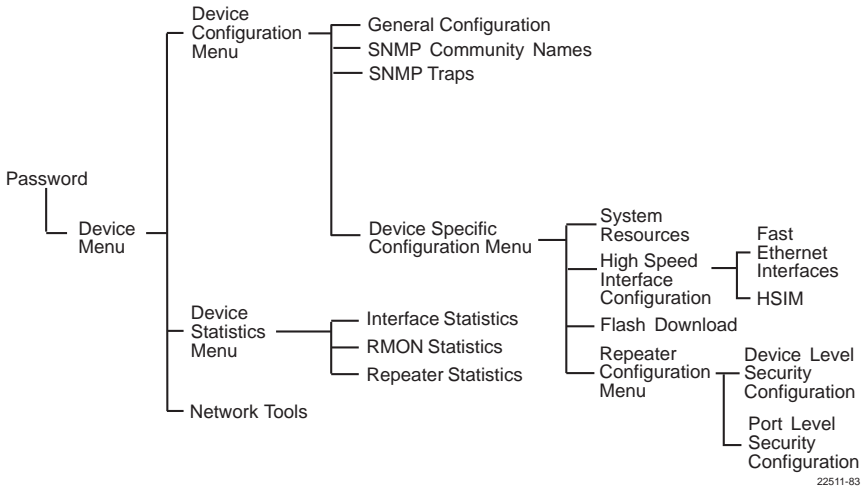


Figure 5-6 SecureFast VLAN Mode, LM Screen Hierarchy

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.

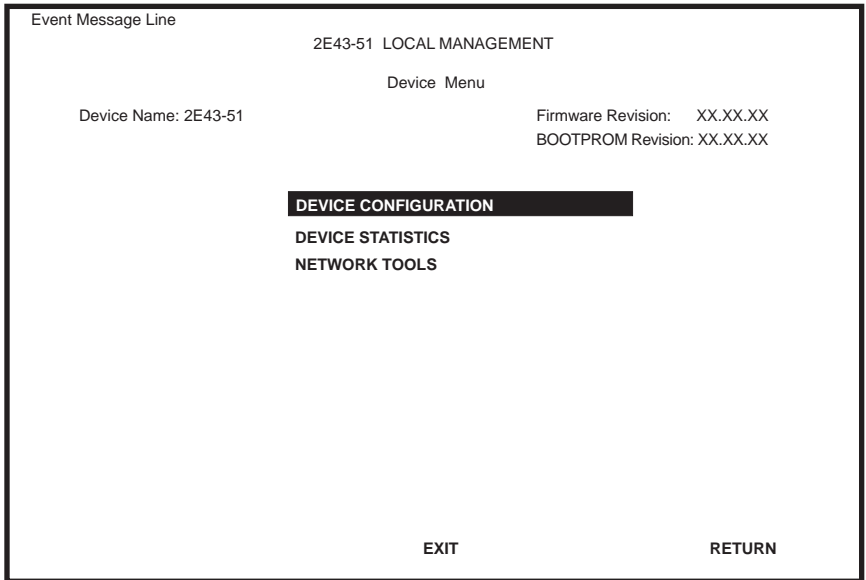


The user can also exit Local Management screens by pressing ESC twice. This exit method does not warn about unsaved changes and all unsaved changes are lost.

3. Exit from 2E43-51 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.

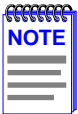
5.5 DEVICE MENU SCREEN

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



2251_13

Figure 5-7 Device Menu Screen



If the terminal is idle for several minutes, the Local Management Password screen redisplay and the session ends.

The following explains each Device Menu screen field as shown in [Figure 5-7](#):

DEVICE CONFIGURATION

The Device Configuration screen provides access to the Local Management screens that are used to configure the 2E43-51 and also to the Device Specific Configuration Menu screen. The Device Specific Configuration Menu screen provides access to the screens that allow the user to check the 2E43-51 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 5.11](#).

DEVICE STATISTICS

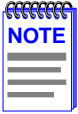
The Device Statistics screen provides statistics and performance information for the 2E43-51. For details, refer to [Section 5.21](#).

NETWORK TOOLS

The Network Tools function resides on the 2E43-51 and consists of a series of commands that allow the user to access and manage network devices. [Section 5.26](#) explains how to use the Network Tools utility.

5.6 DEVICE CONFIGURATION MENU SCREEN

The Device Configuration Menu screen, [Figure 5-8](#), provides access to Local Management screens. These screens allow the user to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, configure switch parameters and configure 2E43-51 ports.



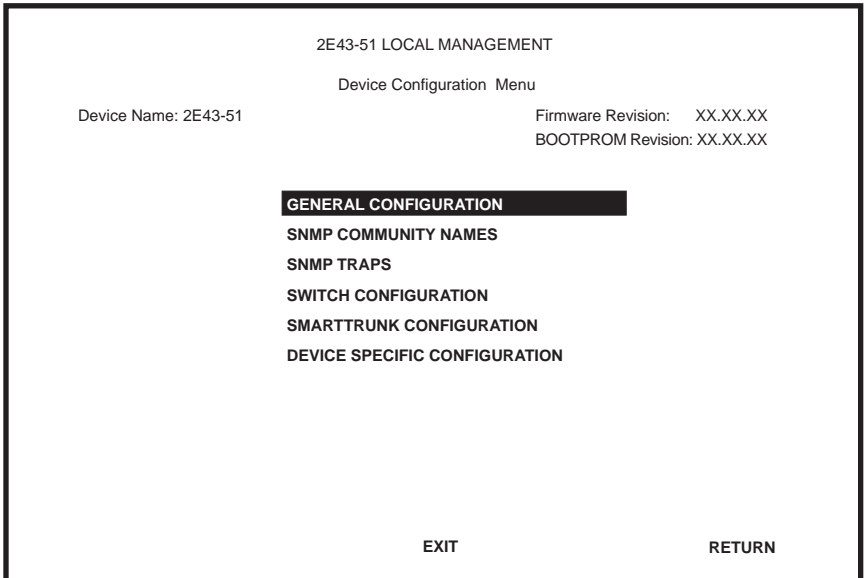
The following menu items on the Device Configuration Menu screen do not display if the operational mode of the device is set to SECURE FAST VLAN:

SWITCH CONFIGURATION

SMARTTRUNK CONFIGURATION

[Section 5.7.9](#) provides instructions on setting the operational mode.

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.



22511_66

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 the user to monitor and configure operating parameters for the 2E43-51. For details, refer to [Section 5.7](#).

SNMP COMMUNITY NAMES

The SNMP Community Names screen allows the user to enter new, change, or review the community names used as access passwords for device management operation. Access is limited based on the password level of the user. 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](#).

SMARTTRUNK CONFIGURATION

The SmartTrunk Configuration screen allows the user to logically group interfaces to aggregate high speed uplinks. For details, refer to the *SmartTrunk User's Guide*.

DEVICE SPECIFIC CONFIGURATION

The Device Specific Configuration Menu screen allows the user to select screens to configure ports or check system resources specific to the 2E43-51. For details, refer to [Section 5.11](#).

5.7 GENERAL CONFIGURATION SCREEN

The General Configuration screen, [Figure 5-9](#), allows the user to set the system date and time, IP address and subnet mask, the Default Gateway, the TFTP Gateway IP address, and the operational mode. Also, clear the NVRAM, set the screen refresh time, the screen lockout time, the IP fragmentation, and the COM port configuration.

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.

Event Message Line			2E43-51 LOCAL MANAGEMENT		
General Configuration					
Device Name: 2E43-51			Firmware Revision: XX.XX.XX BOOTPROM Revision: XX.XX.XX		
MAC Address:	00-00-ID-00-00-00	Device Date:	01/11/1997		
IP Address:	0.0.0.0	Device Time:	14:23:00		
Subnet Mask:	0.0.0.0	Screen Refresh Time:	03 sec.		
Default Gateway:	NONE DEFINED	Screen Lockout Time:	15 min.		
TFTP Gateway IP Addr:	0.0.0.0	Device Uptime:	XX D XX H XX M		
Operational Mode: [Switching]					
Com: [ENABLED]	Application:		[LM]		
Clear NVRAM: [NO]	IP Fragmentation		[ENABLED]		
SAVE	EXIT			RETURN	

2251-15

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 2E43-51.

IP Address (Modifiable)

Displays and allows the user to set the IP address for the 2E43-51. 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 1.3.5](#).

Subnet Mask (Modifiable)

Displays the subnet mask for the 2E43-51. 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 2E43-51. This field is not defined until an appropriate value is entered. For details about why and how to set the Default Gateway, refer to [Section 5.7.3](#).

TFTP Gateway IP Addr (Modifiable)

Displays and allows the user to set the TFTP Gateway IP address for the 2E43-51. To set the TFTP Gateway IP address, refer to [Section 5.7.4](#).

Device Date (Modifiable)

Contains a value that the device 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 module's screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified module'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 Local Management 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 (Selectable)

Allows the user to set the 2E43-51 so it operates as a an 802.1D switch (802.1D SWITCHING), an IEEE 802.1Q switch (802.1Q SWITCHING), or a Cabletron Systems SecureFast switch (SECURE FAST VLAN).

In 802.1D SWITCHING mode, the 12 connections on each RJ21 port (ENET1 – ENET4) act as repeaters, and may be switched to each other and to any Fast Ethernet Interface Module and HSIM port(s) in the 2E43-51R.

In 802.1Q SWITCHING mode, the device is able to increase its switching functionality by creating and maintaining IEEE 802.1Q port based Virtual LANs (VLANs).

When the operational mode is set to SECURE FAST VLAN, the device acts as a SecureFast switch. With the Cabletron Systems VLAN Manager software, the device is able to increase its switching functionality by creating and maintaining VLANs.

For details on how to select the Operational Mode, refer to [Section 5.7.9](#).

Com (Toggle)

Allows the user 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 (Toggle)

Allows the user to set the application that the COM port supports. The field toggles between LM (Local Management) and UPS (Uninterruptible Power Supply).

The UPS setting allows the COM port to be used to monitor an American Power Conversion (APC) Uninterruptible Power Supply (UPS).

The baud rate setting for LM is automatically sensed. For UPS, the baud rate is automatically set to 2400.

The default setting is LM. For details about how to configure the COM port for various applications, refer to [Section 5.7.10](#).

Clear NVRAM (Toggle)

Allows the user to reset NVRAM to the factory default settings. All user-entered parameters, such as IP address and Community Names, are then replaced with 2E43-51 default configuration settings. For details, refer to [Section 5.7.11](#).

IP Fragmentation (Toggle)

Allows the user to enable or disable IP Fragmentation. The default setting for this field is ENABLED. If the 2E43-51 is to be bridged to an FDDI ring, IP Fragmentation must be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size are discarded. For details on enabling IP Fragmentation, refer to [Section 5.7.12](#).

5.7.1 Setting the IP Address

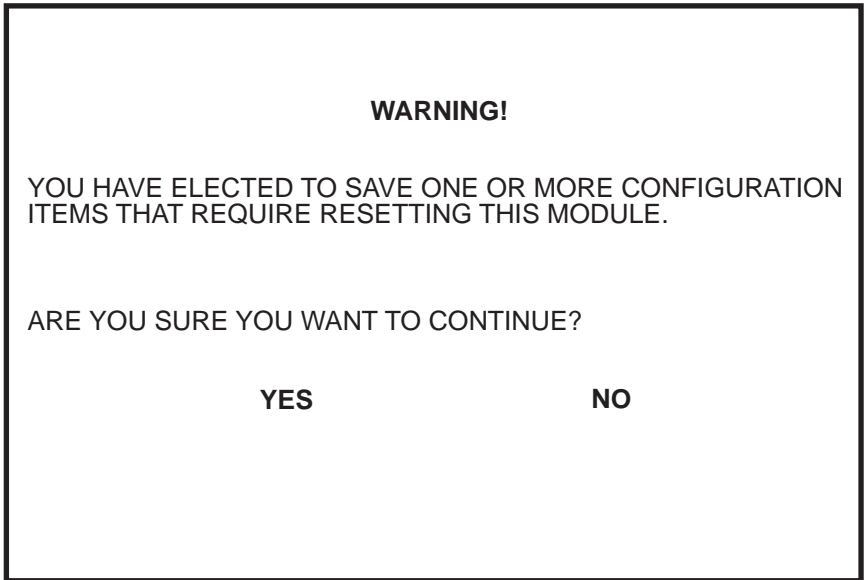
To set the IP address, perform the following steps:

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Dotted Decimal 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 screen displays the message “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.



19601-84

Figure 5-10 Configuration Warning Screen

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

5.7.2 Setting the Subnet Mask

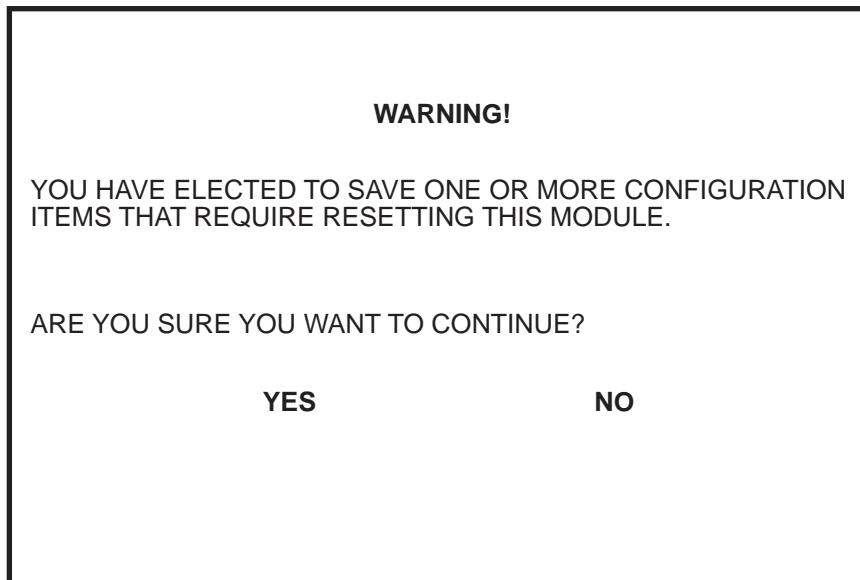
If the management workstation that is to receive SNMP traps from the 2E43-51 is located on a separate subnet, the subnet mask for the 2E43-51 may need to be changed from its default.

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 Dotted Decimal Notation (DDN) format.

For example: 255.255.0.0

3. Press ENTER. If the subnet mask 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 5-11 displays.



19601-84

Figure 5-11 Configuration Warning Screen

5. Use the arrow key to highlight the **YES** command, then press ENTER. The changes are saved and the device reboots.

5.7.3 Setting the Default Gateway

If the SNMP management station is located on a different IP subnet than the 2E43-51, a default gateway must be specified. When an SNMP Trap is generated, the 2E43-51 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 2E43-51, a Gateway IP address should be specified. To set the TFTP Gateway IP address, perform the following steps:

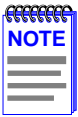
1. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
2. Enter the IP address of the TFTP gateway using the DDN format.
For example: 134.141.80.122
3. Press ENTER. If the TFTP gateway IP address entered is a valid format, the cursor returns to the beginning of the TFTP Gateway IP Address field. If the entry is not valid, the screen displays “INVALID TFTP GATEWAY IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the TFTP Gateway IP Address 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.

5.7.5 Setting the Device Date

The 2E43-51 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 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, but it does refresh the Device Date 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 from 3 to 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 can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

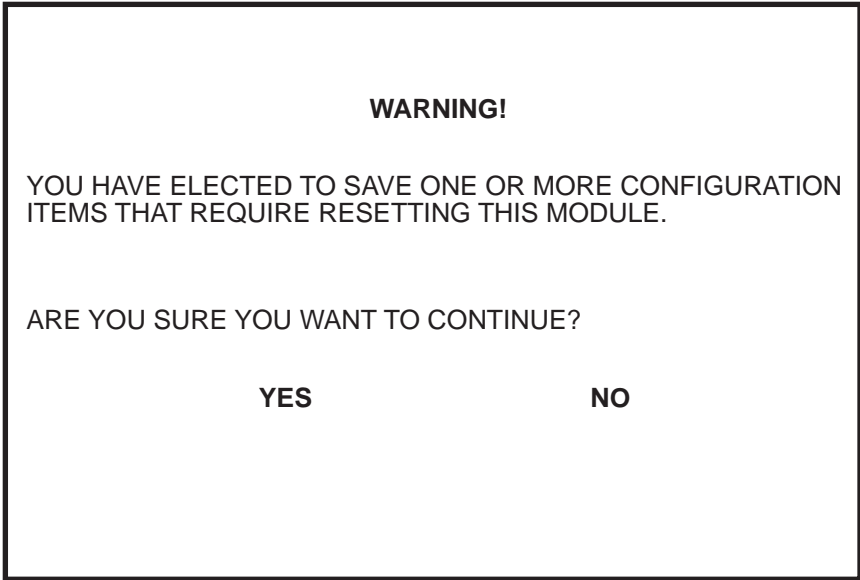
1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes 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

To set the Operational Mode, proceed as follows:

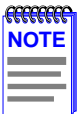
1. Use the arrow keys to highlight the **Operational Mode** field.
2. Press the SPACE bar to toggle to the appropriate operational mode (**802.1D SWITCHING**, **802.1Q SWITCHING** or **SECURE FAST VLAN**).
3. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown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



19601-84

Figure 5-12 Configuration Warning Screen

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



If the 2E43-51 is 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 2E43-51 is 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, the user must enable/disable the COM port and select an application.

The 2E43-51 COM port supports the following applications:

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

To configure the COM port, proceed as follows:

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

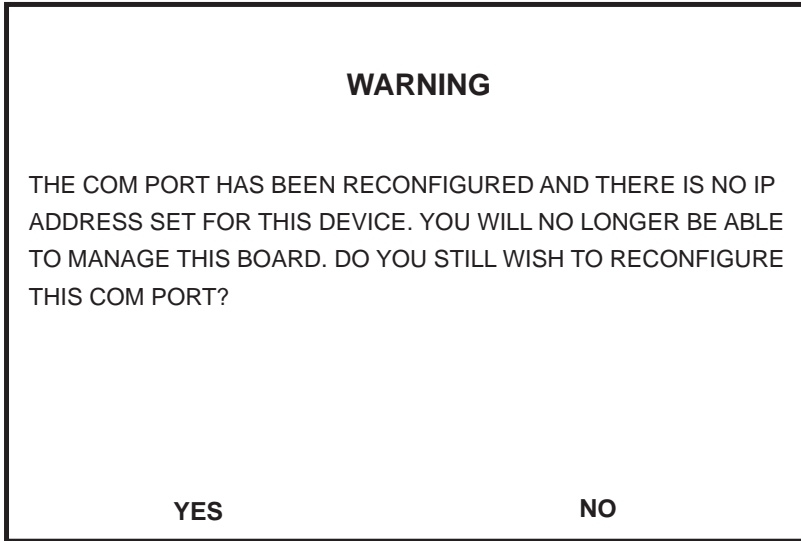


Do **NOT** disable or alter the settings of the COM port while operating the current Local Management connection through a terminal. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session. If the 2E43-51 was previously assigned a 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 2E43-51 (refer to [Section 5.7.11](#)) to reestablish COM port communications.

2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**. **ENABLED** supports the connection of a terminal to the COM port for a particular application. **DISABLED** does not support the connection of a terminal to the COM port.



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.



174252

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**” appears, the edits you made are saved.



Exiting without saving causes the message “**NOT SAVED -- PRESS SAVE TO KEEP CHANGES**” to appear. Exiting without saving causes all edits to be lost.

6. Use the arrows keys to highlight the **Application** field.

- Use the SPACE bar or BACKSPACE to step through the available settings until the operation you require appears. 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

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

5.7.11 Clearing NVRAM



Clearing NVRAM will result in the loss of all user-entered parameters. Do not proceed unless this procedure is completely understood.

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

Clear NVRAM as follows:

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

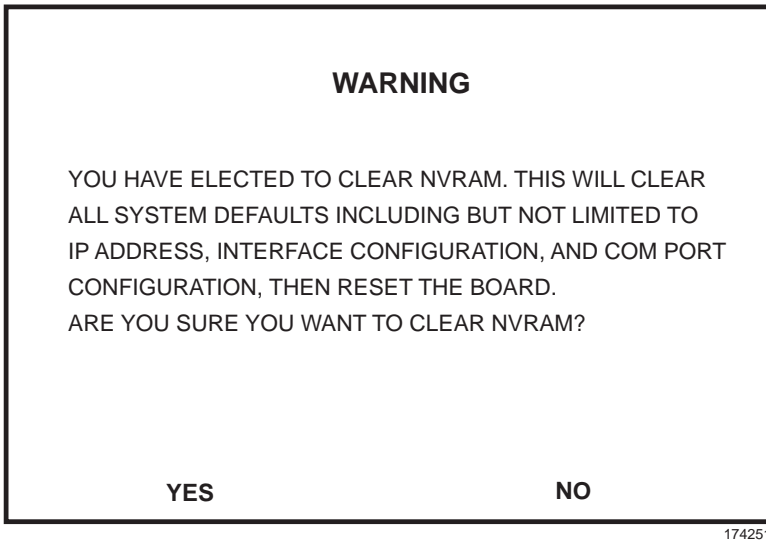


Figure 5-14 Clear NVRAM Warning Screen

5. Select **YES** and the message “CLEARING NVRAM. REBOOT IN PROGRESS...” displays.
6. The 2E43-51 clears NVRAM and reboots. All user-entered parameters default to factory default settings.

5.7.12 Enabling/Disabling IP Fragmentation

To enable or disable IP Fragmentation, proceed as follows:

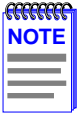


If the 2E43-51 is being bridged to an FDDI ring (for example, via an optional HSIM-F6), enable IP Fragmentation. If it is disabled, all FDDI frames that exceed the maximum Ethernet frame size are discarded.

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

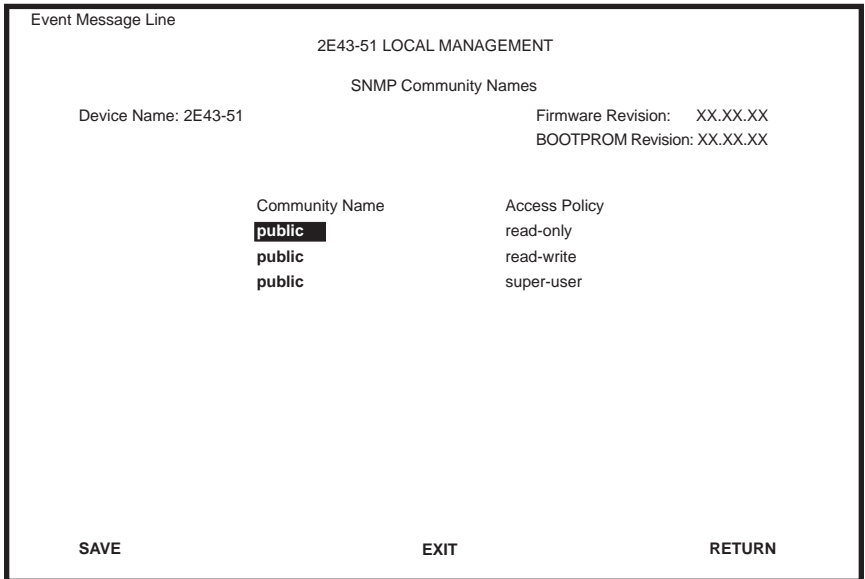
5.8 SNMP COMMUNITY NAMES SCREEN

The SNMP Community Names screen allows the user to set SNMP Management community names. Community names act as passwords to Local/Remote Management and are agents of security access to the 2E43-51. Access to the 2E43-51 is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).



Super-user access gives the user 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 displays.



2251-16

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 2E43-51 SNMP Management. Any community name assigned here acts as a password to Local/Remote Management.

Access Policy (Read-Only)

Indicates the access accorded each community name. The available access levels are as follows:

read-only	This community name gives the user read-only access to the 2E43-51 MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.
read-write	This community name gives the user read-write access to the 2E43-51 MIB objects, excluding security protected fields for Super-User access only.
super-user	This community name gives the user read-write access to the 2E43-51 MIB objects and allows the user 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 at 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 the 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.



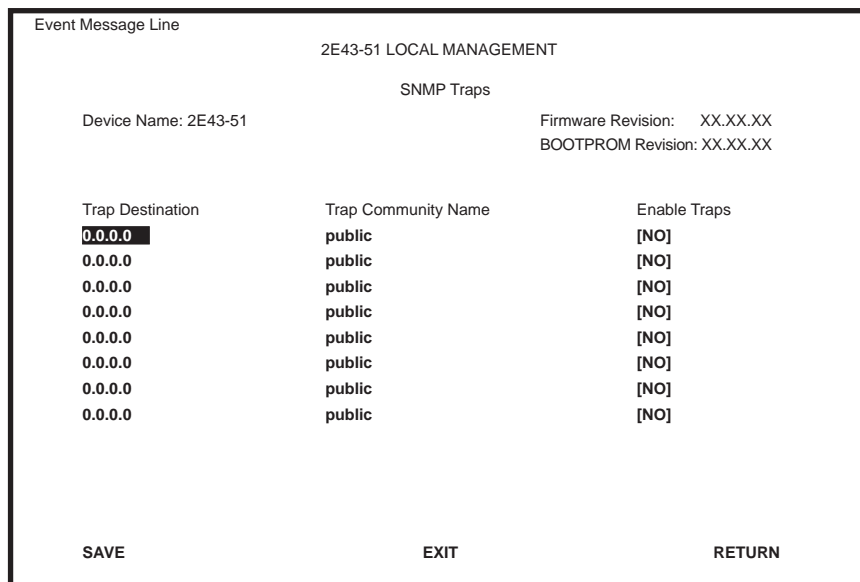
Exiting without saving causes a “NOT SAVED?” message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

6. To exit the screen, use the arrow keys to highlight **RETURN** and press ENTER.

5.9 SNMP TRAPS SCREEN

Since the 2E43-51 is an 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.



2251-17

Figure 5-16 The 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.

Trap Community Name (Modifiable)

Displays the Community Name included in the trap message sent to the Network Management Station with the associated IP address.

Enable Traps (Toggle)

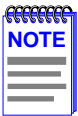
Enables transmission of the traps to the network management station with the associated IP address. This field toggles between YES and NO.

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 2E43-51 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 on the screen.

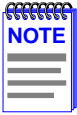


Exiting without saving causes a “NOT SAVED?” message to appear above the **SAVE** command. Edits are lost if they are not saved before exiting.

8. To exit the screen, use the arrow keys to highlight **RETURN** and press ENTER.

The designated workstations now receive traps from the 2E43-51.

5.10 SWITCH CONFIGURATION SCREEN



The Switch Configuration screen is not available if the operational mode of the device is set to SECURE FAST VLAN. This screen may only be used when the device is configured to operate as an 802.1D or 802.1Q switch.

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 up to 7 ports, depending on if there are Fast Ethernet Interface Modules and an HSIM installed in the device.

```
Event Message Line
                                2E43-51 LOCAL MANAGEMENT

                                Switch Configuration

Device Name: 2E43-51                Firmware Revision:  XX.XX.XX
                                BOOTPROM Revision: XX.XX.XX

Switch Address: 00-00-1D-00-00-00   Type of STA:      [DEC]
Number of Ports: 7                  Age Time (sec):  300

Port #      MAC Address             State             Status
-----
1           00-00-1D-00-00-00       learning         [ENABLED]
2           00-00-1D-00-00-01       listening        [DISABLED]
3           00-00-1D-00-00-02       standby          [ENABLED]
4           00-00-1D-00-00-03       learning         [DISABLED]
5           00-00-1D-00-00-04       listening        [ENABLED]
6           00-00-1D-00-00-05       standby          [DISABLED]
7           00-00-1D-00-00-06       listening        [ENABLED]

SAVE                EXIT                RETURN
```

22511-18

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 on the 2E43-51.



Ethernet networks 1 through 4 (ENET 1 through ENET 4) are considered as single switched ports.

Type of STA (Toggle)

Allows the user 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 selection is 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) that the 2E43-51 keeps an address in its switch table before discarding it. An address is automatically discarded when a valid Bridge Protocol Data Unit (BPDU) is not received from that address within the 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 switched port on the device.

MAC Address (Read-Only)

Displays the hardware address assigned to each listed port.

State (Read-Only)

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

Listening: The switch is not adding information to the Transparent Database. The switch is monitoring the Bridge Protocol Data Unit (BPDU) traffic while preparing to move from the learning to the forwarding state.

Learning: The switch is learning the addresses on this interface. The switch enters the learning state when the Transparent Database is created (during start-up or after being deleted), or when the Spanning Tree Algorithm detects a network topology change.

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

Blocking: This interface will not forward any traffic through the switch because a loop condition has been detected by the STA.

Status (Toggle)

Allows the user 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 the user 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 Field

To set the Age Time, proceed as follows:

1. Use the arrow keys to highlight the **Age Time** field.
2. Type in the desired Age Time in increments of 10. The available Age Time range is 10 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” is displayed.

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 DEVICE SPECIFIC CONFIGURATION MENU SCREEN

The Device Specific Configuration Menu screen, [Figure 5-18](#), allows the user to select one of five screens to configure ports or check system resources specific to the 2E43-51.

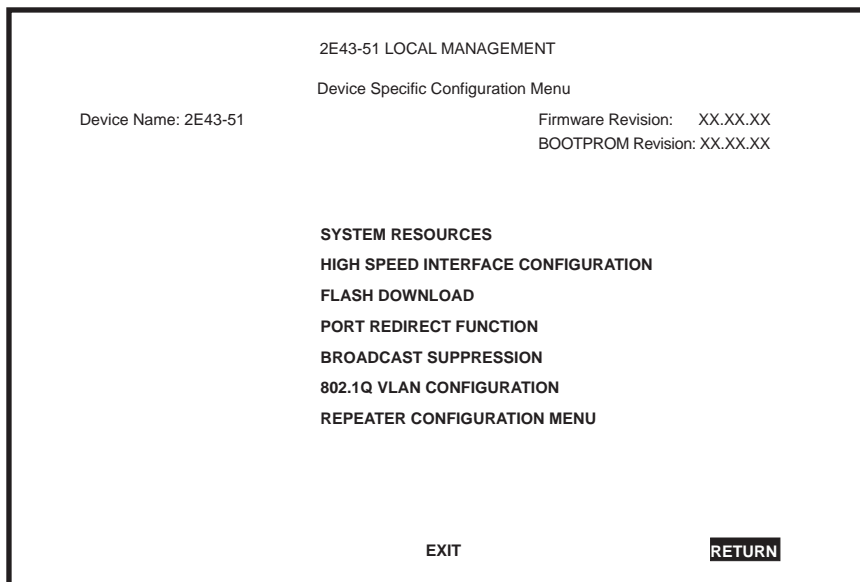


The PORT REDIRECT FUNCTION menu item on the Device Specific Configuration Menu screen does not display if the operational mode of the device is set to 802.1Q SWITCHING.

The PORT REDIRECT FUNCTION and BROADCAST SUPPRESSION menu items do not display if the operational mode is set to SECURE FAST VLAN.

[Section 5.7.9](#) provides instructions on 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 displays.



22513-20

Figure 5-18 Device Specific Configuration Menu Screen

The following explains each selectable item in 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 2E43-51 operation. For details, refer to [Section 5.12](#).

HIGH SPEED INTERFACE CONFIGURATION

The High Speed Interface Configuration screen provides access to the Fast Ethernet Interfaces screen and the HSIM screen. For details, refer to [Section 5.13](#).

FLASH DOWNLOAD

The FLASH Download screen allows the user to download information from FLASH memory and force the 2E43-51 to download a new image file from a TFTP server. For details, refer to [Section 5.15](#).

PORT REDIRECT FUNCTION

The Port Redirect Function screen allows the user to redirect traffic from one or multiple switch ports to a specific destination switch port. For details, refer to [Section 5.16](#).

BROADCAST SUPPRESSION

The Broadcast Suppression screen allows the user to set a desired limit of received broadcast frames that will be forwarded per port per second. For details, refer to [Section 5.17](#).

802.1Q VLAN CONFIGURATION

This menu item will only display if the 2E43-51 has been configured to operate as an 802.1Q switch as described in [Section 5.7.9](#). When selected, this menu item opens the VLAN Main Menu screen. For details about the VLAN Local Management screens, refer to the Cabletron Systems *Port Based VLAN User's Guide*.

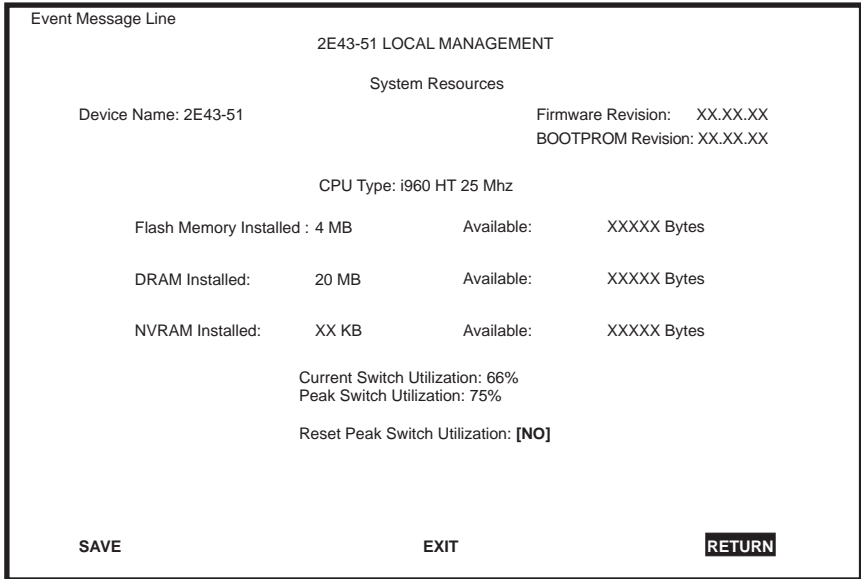
REPEATER CONFIGURATION MENU

The Repeater Configuration Menu screen enables the user to select the security screens: Device Level Security Configuration, and Port Level Security Configuration. For details refer to [Section 5.18](#).

5.12 SYSTEM RESOURCES SCREEN

The System Resources screen, [Figure 5-19](#), provides information concerning the processor used in the 2E43-51 and the amount of FLASH memory, DRAM, and NVRAM that is installed and how much of that memory is available. This screen also allows the user 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.



2251-23

Figure 5-19 System Resources Screen

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

CPU Type (Read-only)

Indicates the microprocessor used in the 2E43-51.

Flash Memory Installed (Read-only)

Indicates the amount of FLASH memory installed in the 2E43-51 and how much is currently available.

DRAM Installed (Read-only)

Indicates the amount of DRAM installed in the 2E43-51 and how much of it is currently available.

NVRAM Installed (Read-only)

Indicates the amount of NVRAM installed in the 2E43-51 and how much of it is currently available.

Current Switch Utilization (Read-only)

Shows the percentage of the device switching capacity currently being used.

Peak Switch Utilization (Read-only)

Shows the peak percentage of device switching capacity used, since the last reset.

Reset Peak Switch Utilization (Toggle)

Allows the user to reset the Peak Switch Utilization field. The switch may be set to either YES or NO as described in [Section 5.12.1](#). YES resets the Peak Switch Utilization field to the current system traffic.

5.12.1 Setting the Reset Peak Switch Utilization

To set the Reset Peak Switch 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 arrows keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.13 HIGH SPEED INTERFACE CONFIGURATION MENU SCREEN

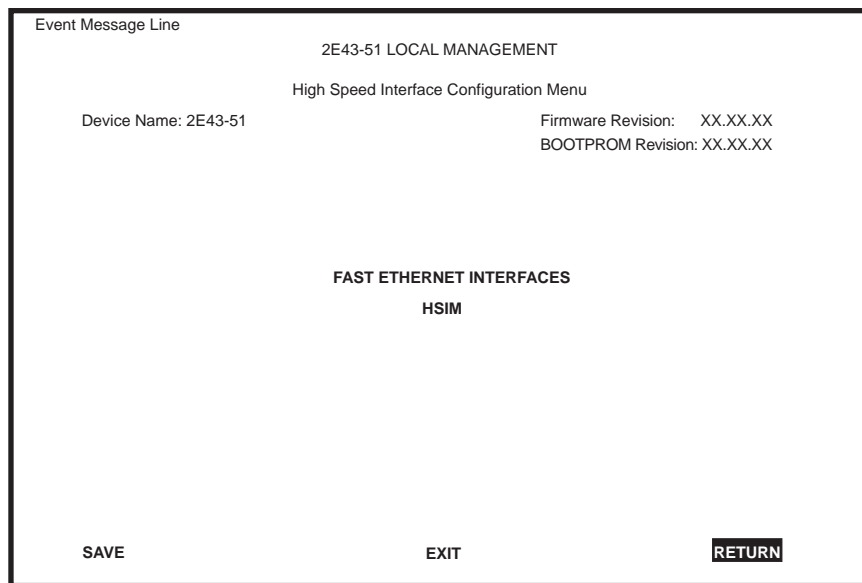
The High Speed Interface Configuration Menu screen, [Figure 5-20](#), applies to the Fast Ethernet Interface Modules and the High Speed Interface Module.



This screen does not display unless one or two Fast Ethernet Interface Modules and a High Speed Interface Module (HSIM) are installed.

If only the Fast Ethernet Interface Module(s) or the HSIM is installed, then the respective Fast Ethernet Interfaces screen or the HSIM Setup screen displays instead of the High Speed Interface Configuration Menu screen.

To access the High Speed Interface Configuration Menu screen from the Device Specific Configuration Menu screen, use the arrow keys to highlight the **HIGH SPEED INTERFACE CONFIGURATION** menu item and press ENTER. The High Speed Interface Configuration Menu screen displays.



22511-53

Figure 5-20 High Speed Interface Configuration Menu Screen

The following briefly explains each screen accessible from the High Speed Interface Configuration Menu screen.

FAST ETHERNET INTERFACES

Displays a screen named High Speed Interface Configuration. This screen shows the types of Fast Ethernet Interface Modules installed in ports 5 and 6, their current operating mode, and indicates if the ports are linked. This screen also allows the user to enable or disable Auto-Negotiation and set the Advertised Ability. For details, refer to [Section 5.14](#).

HSIM

Displays the types of interfaces installed in the High Speed Interface Module (HSIM) slots. The HSIM screens are described in their respective user's guides.

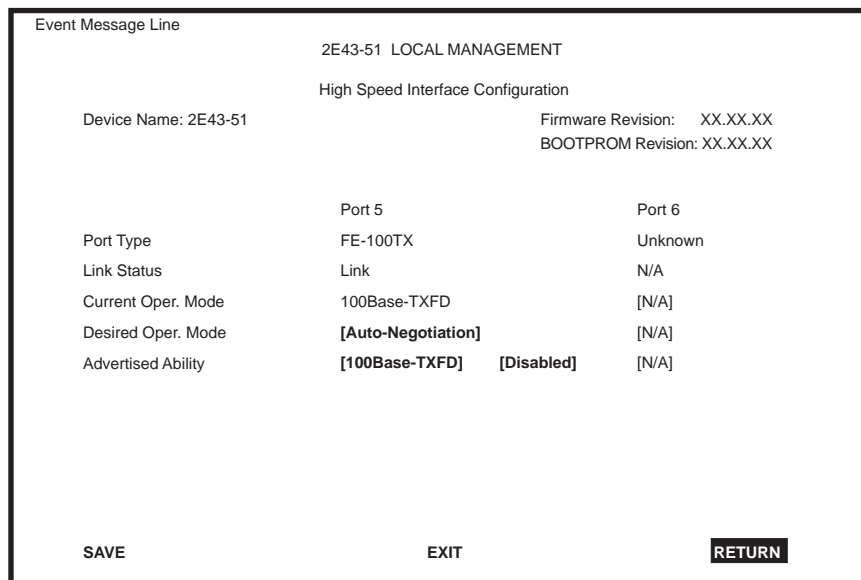
5.14 HIGH SPEED INTERFACE CONFIGURATION SCREEN



The High Speed Interface Configuration screen, [Figure 5-21](#), applies only to ports 5 and 6. This screen supports the FE-100TX, FE-100FX, and FE-100F3 Fast Ethernet Interface Modules that operate at 100 Mbps.

The High Speed Interface Configuration screen displays the types of interfaces installed in ports 5 and 6, their current operating mode, and indicates if the ports are linked. This screen also allows the user to enable or disable Auto-Negotiation and set the Advertised Ability.

To access the High Speed Interface Configuration screen from the High Speed Interface Configuration Menu screen, use the arrow keys to highlight the **FAST ETHERNET INTERFACES** menu item and press ENTER. The High Speed Interface Configuration screen displays.



2251-24

Figure 5-21 High Speed Interface Configuration Screen

The following briefly explains each field of the High Speed Interface Configuration screen.

Port Type (Read-only)

Displays the type of interface (FE-100FX, FE-100TX, FE-100F3, or Unknown) installed in ports 5 and 6. [Figure 5-21](#) shows that there is an FE-100TX interface installed in port 5 and no interface indicated by Unknown in port 6.

Link Status (Read-only)

Indicates whether or not there is a physical connection from this port to another 10BASE-T or 100BASE-TX/FX device. One of the following values displays:

- **Link** – There is a link signal present and a valid physical connection to another device.
- **No Link** – There is no link signal present and no valid physical connection to another device.

Current Oper. Mode (Read-only)

This field displays the current operating mode of ports 5 and 6. Depending on whether a 100BASE-FX or 100BASE-TX Fast Ethernet Interface Module is installed, this field displays the following:

- With a 100BASE-FX interface: 100Base-FX, 100Base-FXFD (full duplex), or N/A when the port slot is empty.
- With a 100BASE-TX interface: Unknown, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, 100Base-TXFD (full duplex) or N/A when the port slot is empty.

Desired Oper. Mode (Selectable)

This field allows the user to select the desired operational mode for an interface in port 5 or 6. The field toggles between 100Base-FX and 100Base-FXFD (full duplex) when an FE-100FX or FE-100F3 is installed. [Section 5.14.1](#) describes how to configure a port with an FE-100FX or FE-100F3.



In normal operation, the port with an FE-100TX installed automatically establishes a link with the device at the other end of the segment without requiring user setup. However, Local Management provides the user with the option of manually configuring that port.

If an FE-100TX is installed, the field steps to Auto-Negotiation, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex). In normal operation, the port with an FE-100TX installed is capable of auto-negotiating the operational mode and no further user setup is required. [Section 5.14.2](#) describes how to manually configure an FE-100TX.

In Auto Negotiation, the FE-100TX negotiates to the highest common denominator of the two interfaces. The order of priority of negotiation is 100Base-TXFD, 100Base-TX, 10Base-TFD, and 10Base-T.

Advertised Ability (Selectable)

During auto-negotiation, the FE-100TX “tells” the device at the other end of the segment about its capabilities. The capabilities of a port (5 or 6) 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 5.14.2.2](#) describes how to enable or disable advertised modes.

5.14.1 Configuring an FE-100FX or FE-100F3

When an FE-100FX or FE-100F3 is installed in port 5 or 6, it must be manually set to operate in the same technology as the device at the other end of the connected segment. [Section 5.14.1.1](#) provides instructions for manually configuring the port with an FE-100FX or FE-100F3 interface.

5.14.1.1 Setting the FE-100FX or FE-100F3 Operational Mode

Use the Desired Oper. Mode 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 Oper. 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.

5.14.2 Configuring an FE-100TX

In normal operation, a port (5 or 6) 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 5.14.2.1](#) and [Section 5.14.2.2](#) provide instructions for manually configuring the port with an FE-100TX installed.

5.14.2.1 Setting the FE-100TX Operational Mode

Use the Desired Oper. Mode field to set the active technology. This field steps between 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 is displayed in both the Desired Operational Mode field and the Current Operational Mode field.

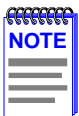
5.14.2.2 Setting the FE-100TX Advertised Ability

In normal operation, a port (5 or 6) with 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. The Advertised Ability field provides the capability to set those 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 arrow keys to move to the **Enable/Disable** field at the right of the desired mode and use the SPACE bar to select **Enabled** or **Disabled**. Press ENTER.
4. Continue this process until you have completed enabling or disabling the advertised modes.
5. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the changes to memory.

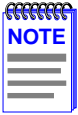
5.15 FLASH DOWNLOAD SCREEN

The Flash Download screen, shown in [Figure 5-22](#), allows the user to upgrade the device with a different operating image.



The user may also force the download of an image by changing the position of Switch 6 located inside the device. For details about setting the switch, refer to [Section C.2.1](#).

Before downloading an image to the device, copy the image to the network TFTP server.



For information on how to set up 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.

```
TFTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS...
2E43-51 LOCAL MANAGEMENT

Flash Download

Device Name: 2E43-51                               Firmware Revision:  XX.XX.XX
                                                    BOOTPROM Revision: XX.XX.XX

Download Method:  [TFTP]
Reboot After Download:  [YES]
TFTP Gateway IP Addr:  134.141.79.123
Last Image Server IP:  134.141.79.121
Last Image File Name:  /ftpboot/2E43.hex
Download Server IP:    134.141.79.121
Download File Name:    /ftpboot/2E43.hex

EXECUTE                               EXIT                               RETURN
```

2251-49

Figure 5-22 Flash Download Screen



Download Server IP and Download File Name display 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 device 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 2E43-51 attempts a TFTP download based on the IP address and file name entered in the fields at the bottom of the Flash Download screen. [Section 5.15.1](#) describes how to download using BootP. [Section 5.15.2](#) describes how to download using TFTP. [Section 5.15.3](#) describes how to download using Runtime.

Reboot After Download (Modifiable only when RUNTIME is chosen)

This field notifies the user that the 2E43-51 will reboot after the download is complete. If a Runtime Download is performed, this field toggles between YES and NO. If YES is selected, the device reboots after the download is completed. If NO is selected, the device continues using the existing firmware image and stores the new firmware image in FLASH memory. When the device is reset or during the next power-up, the device will boot 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, Setting the TFTP Gateway IP Address](#).

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 is selected as the download method (see [Figure 5-22](#)), the following two additional fields display:

Download Server IP (Selectable)

The IP address of the TFTP server to be used for the FLASH download is entered in this field.

Download File Name (Selectable)

The complete TFTP Server path and file name of the new image is entered in this field.

5.15.1 Image File Download Using BootP

To download a firmware image of FLASH to the 2E43-51 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.

5.15.2 Image File Download Using TFTP

To download a firmware image of FLASH to the 2E43-51 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 as that 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/2E43.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.

5.15.3 Image File Download Using Runtime

To download a firmware image of FLASH to the 2E43-51 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 or 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/2E43.flb**
11. 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.

5.16 PORT REDIRECT FUNCTION SCREEN



The Port Redirect Function screen can only be 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 5-23](#), allows the user to set each network port (ENET 1 through 4, port 5, and port 6) as a source or destination port. (ENETs 1 through 4 are shown as 1 through 4 on the screen.) A port can be set to have one or more destination ports. For example, port 1 can be set as a source port with three destinations, ports 2, 3, and 4. Traffic from port 1 is then automatically redirected to ports 2, 3, and 4. Port 1 can also serve as a destination port for other ports.

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



Although all traffic from the source port (including, if desired, errored 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.

Event Message Line

2H43-51 LOCAL MANAGEMENT

Port Redirect Function

Device Type: 2H43-51

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

<u>Source Port:</u>	<u>Destination Port:</u>	<u>Remap Errors:</u>
1	2	ON
1	3	ON
1	4	ON
2	1	OFF
2	3	OFF
3	4	ON
3	5	ON
3	6	ON

Source Port [1] Destination Port [1] Errors [ON] Status [ADD]

SAVE NEXT PREVIOUS EXIT **RETURN**

22511_22

Figure 5-23 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. To display the ports, refer to [Section 5.16.1](#).

Destination Port (Read-only)

Shows which ports are currently set as destination ports.

Remap Errors (Read-only)

Displays whether the corresponding source ports are configured (ON) to send errored frames to the destination ports, or (OFF) to drop all errored frames and only forward traffic without errored frames to the destination ports.

Source Port [n] (Selectable)

Allows a selected port [n] to be changed to a source port.

Destination Port [n] (Selectable)

Allows a selected port [n] to be changed to a destination port.

Errors (Toggle)

Allows the user to configure the source ports to either (ON) send errored frames to selected destination ports, or (OFF) drop errored frames, and send only valid traffic to the destination ports. The default setting of this field is ON. To set the Errors field, refer to [Section 5.16.2](#)

Status (Toggle)

Allows the addition or deletion of source and destination ports selected in the Source port [n] and Destination port [n] fields.

5.16.1 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 10 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 displays at the bottom of the first screen. In the second screen, the NEXT and PREVIOUS commands display. 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 displays.

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

5.16.2 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.



To redirect more than one port, repeat steps 1 through 6 for each additional setting, then go to step 7 to save all the new settings at once.

7. 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 Port and Destination Port read-only fields.

5.17 BROADCAST SUPPRESSION SCREEN

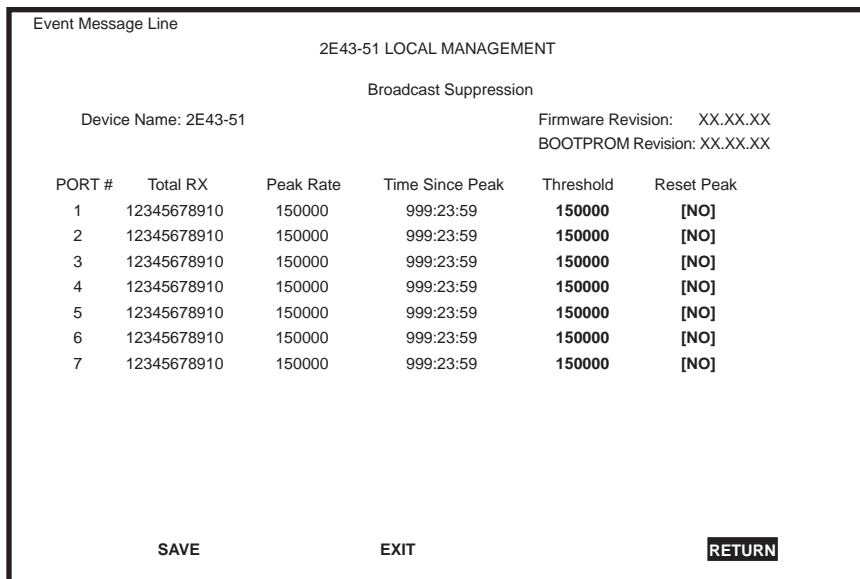
The Broadcast Suppression screen, [Figure 5-24](#), allows the user to set a desired limit of receive broadcast frames that are switched out to the other ports.



The Broadcast Suppression screen is not available if the operational mode of the device is set to SECURE FAST VLAN. This screen may only be used when the device is configured to operate as an 802.1D or 802.1Q switch.

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.



The screenshot shows the Broadcast Suppression screen for device 2E43-51. It displays device name, firmware revision, and bootprom revision. Below this is a table with 7 columns: PORT #, Total RX, Peak Rate, Time Since Peak, Threshold, and Reset Peak. The table lists 7 ports, all with a Total RX of 12345678910, a Peak Rate of 150000, and a Time Since Peak of 999:23:59. The Threshold for all ports is 150000, and the Reset Peak status is [NO]. At the bottom of the screen are three buttons: SAVE, EXIT, and RETURN.

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]

2251-56

Figure 5-24 Broadcast Suppression Screen

The following explains each field of the Broadcast Statistics 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 the user to set the desired limit of receive broadcast frames that will be forwarded per port per second.

Reset Peak (Toggle)

Allows the user 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.

5.17.1 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.

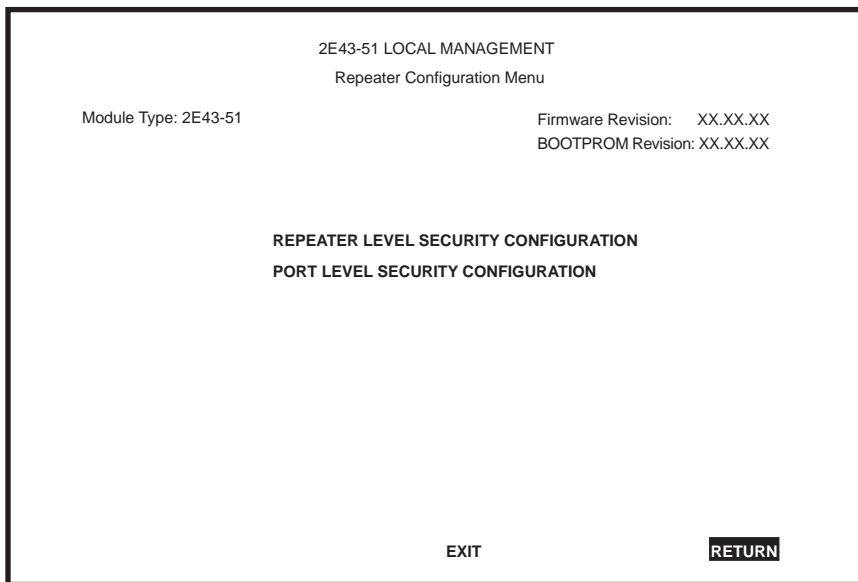
5.17.2 Setting the Reset Peak

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.

5.18 REPEATER CONFIGURATION MENU SCREEN

The Repeater Configuration Menu screen, [Figure 5-25](#), is used to access the Repeater Level Security Configuration, or Port Level Security Configuration screen. To access the Repeater Configuration Menu screen from the Device Specific Configuration Menu screen, select the **REPEATER CONFIGURATION MENU** item and press ENTER. The Repeater Configuration Menu screen displays.



2251_104

Figure 5-25 Repeater Configuration Menu Screen

The following introduces each screen that is accessible from the Repeater Configuration Menu.

REPEATER LEVEL SECURITY CONFIGURATION

Used to set the state of security for each port of a connector simultaneously. The ports can be set to receive all frames (NonSecure state), lock on the source address of the next frame received (LockOnNext) or lock on the address of the last frame received (LockedOnAddr). For details, refer to [Section 5.19](#).

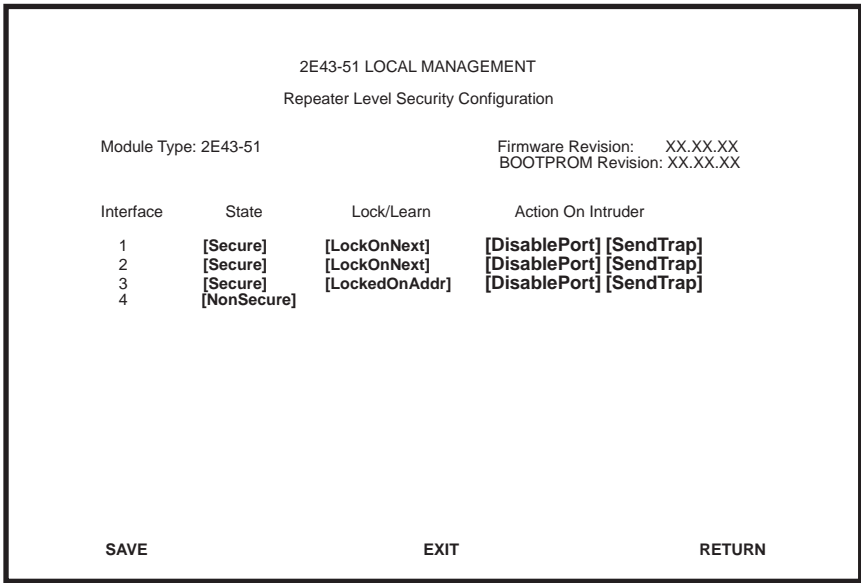
PORT LEVEL SECURITY CONFIGURATION

Used to set the security for each port of a connector, individually. For details, refer to Section 5.20.

5.19 REPEATER LEVEL SECURITY CONFIGURATION

The Repeater Level Security Configuration screen, Figure 5-26, is used to set the state of security for all ports on a connector. A connector can be set to receive all frames (NonSecure state), lock on the source address of the next frame received (LockOnNext), or lock on the source address of the last frame received (LockedOnAddr). When either of the last two options are set, the switch can be set to receive or not receive frames and to send or not send traps when an intruder is detected.

To access the Repeater Level Security Configuration screen, use the arrow keys to highlight the **REPEATER LEVEL SECURITY CONFIGURATION** menu item on the Repeater Configuration Menu screen and press ENTER. The Repeater Level Security Configuration screen displays.



2251_112

Figure 5-26 Repeater Level Security Configuration Screen

The following section defines the fields on the Repeater Level Security Configuration screen.

Interface (Read-Only)

Indicates the repeater port on the ENET connector (ENET 1 through 4) selected in the Interface field. Refer to [Table 5-4](#) for the ENET/repeater port relationship on the device.

Table 5-4 ENET/Repeater Port Relationship

ENET 1 = Repeater ports 1 – 12	ENET 3 = Repeater ports 25 – 36
ENET 2 = Repeater ports 13 – 24	ENET 4 = Repeater ports 37 – 48

State (Selectable)

Used to select the state of security for frames received by any port on the connector. The states are as follows:

- **Secure** – Allows the ports on the connector to receive only those frames with the address as determined by the selection in the Lock/Learn field.
- **NonSecure** – Allows the ports on the connector to receive all frames. The source address of received frames is not examined and the frames are processed in a non secure state.

Lock/Learn (Selectable)

Used to select the type of security for frames received by any port on the connector. The security types are as follows:

- **LockOnNext** – The next frame received by each port is examined to learn its source address. As the source address of a frame is learned on a port, only those frames received with that same source address are processed on that port. Any other address detected is considered as an intruder and the device executes the actions selected in the Action On Intruder field.

- **LockedOnAddr** – The source address of the last frame received (or the source address entered in the Port Level Security Configuration screen, if one is entered) is used for security purposes. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field.

Action On Intruder (Toggle)

Used to select the actions taken for the selected security state. There are two fields to select the actions. Both toggle to activate or deactivate the action.

- **DisablePort/NoDisable** – **DisablePort** causes the switch to turn off the port that had a security violation. With **NoDisable** set, the port is not turned off.
- **SendTrap/NoTrap** – **SendTrap** causes the switch to send an SNMP trap when a port detects a security violation. With **NoTrap** set, no SNMP trap is sent.

5.19.1 Setting the Repeater Level Security

To set the repeater security for each connector, proceed as follows:

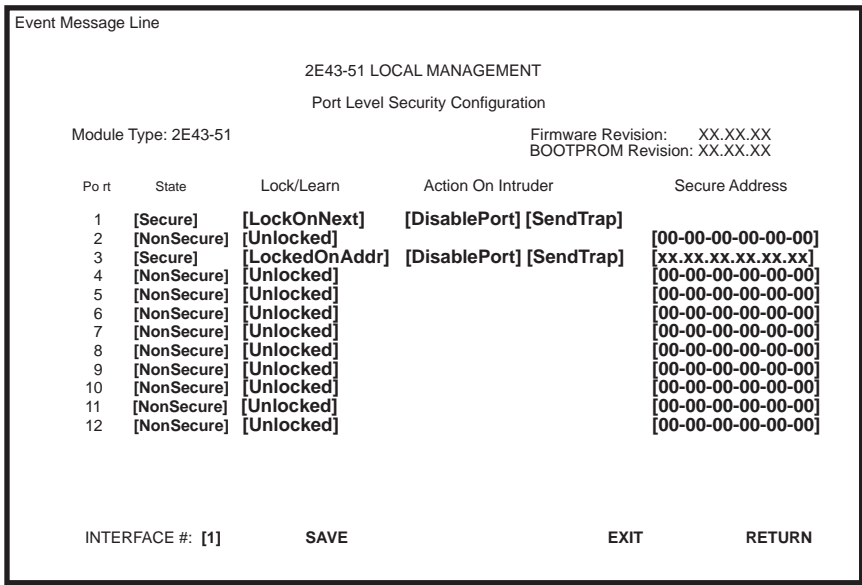
1. Use the arrow keys to highlight the **STATE** field for the interface connector.
2. Use the SPACE bar to step to the appropriate security level (Secure or NonSecure).
3. Use the arrow keys to highlight the **Lock/Learn** field for the connector.
4. Use the SPACE bar to step to the appropriate type of security (LockOnNext or LockedOnAddr).
5. If the security level chosen causes the **DisablePort** and **SendTrap** fields to display under Action On Intruder, use the arrow keys to highlight the **DisablePort** field. If the security level chosen does not cause the fields to display under Action On Intruder, proceed to step 9.
6. To change the **DisablePort** setting to **NoDisable**, press the SPACE bar to toggle the setting.

7. Use the arrow keys to highlight the **SendTrap** field.
8. To change the **SendTrap** setting to **NoTrap**, press the SPACE bar to toggle the setting.
9. To change the security on more than one connector, repeat steps 1 through 8 for each connector. Then proceed to step 10 to save all settings at once.
10. Use the arrow keys to highlight the **SAVE** command.
11. Press ENTER. The message “SAVED OK” displays and all ports of the connector are set to the selected operating mode.

5.20 PORT LEVEL SECURITY CONFIGURATION SCREEN

The Port Level Security Configuration screen, [Figure 5-27](#), functions similarly to the Repeater Level Security Configuration screen, except that it is used to set the security of each port of a connector.

To access the Port Level Security Configuration screen, use the arrow keys to highlight the **PORT LEVEL SECURITY CONFIGURATION** menu item on the Repeater Configuration Menu screen and press ENTER. The Port Level Security Configuration screen displays.



2251_113

Figure 5-27 Port Level Security Configuration Screen

The following section defines the fields on the Port Level Security Configuration screen.

Port (Read-only)

Indicates the repeater port on the ENET connector (ENET 1 through 4) selected in the INTERFACE # field. Refer to Table 5-5 for the connector/repeater port relationship on the device.

Table 5-5 ENET/Repeater Port Relationship

ENET 1 = Repeater ports 1 – 12	ENET 3 = Repeater ports 25 – 36
ENET 2 = Repeater ports 13 – 24	ENET 4 = Repeater ports 37 – 48

State (Selectable)

Used to select the state of security for frames received by any port on the connector. The states are as follows:

- Secure – Allows the ports on the connector to receive only those frames with the address as determined by the selection in the Lock/Learn field.

- **NonSecure** – Allows the ports on the connector to receive all frames. The source address of received frames is not examined and the frames are processed in a non secure state.

Lock/Learn (Selectable)

Used to select the type of security for frames received by any port on the connector. The security types are as follows:

- **LockOnNext** – The next frame received by each port is examined to learn its source address. As the source address of a frame is learned on a port, only those frames received with that same source address are processed on that port. As each port is locked on the next address, the device executes the actions selected in the Action On Intruder field.
- **LockedOnAddr** – The source address of the last frame received (or the source address entered in the Port Level Security Configuration screen, if one is entered) is used for security purposes. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field.

Action On Intruder (Toggle)

Used to select the actions taken for the selected security state. There are two fields to select the actions. Both toggle to activate or deactivate the action.

- **DisablePort/NoDisable** – **DisablePort** causes the switch to turn off the port that had a security violation. With **NoDisable** set, the port is not turned off.
- **SendTrap/NoTrap** – **SendTrap** causes the switch to send an SNMP trap when a port detects a security violation. With **NoTrap** set, no SNMP trap is sent.

Secure Address (Modifiable)

Used to enter the source address for the LockedOnAddr security state setting. Once a secure address is defined on a port, only those frames received with that same source address are processed on that port. Any other frame detected with a different address is considered as an intruder, causing the device to execute the actions selected in the Action On Intruder field. When the security state setting is NonSecure, the field displays the source address of the last frame.

INTERFACE # (Selectable)

This command field selects the front panel interface connector (ENET 1 to ENET 4) to which the port security settings will be applied.

5.20.1 Setting the Port Level Security

To set the security for each repeater port on a connector, proceed as follows:

1. Use the arrow keys to highlight the **INTERFACE #** field.
2. Use the SPACE bar to step to the appropriate interface connector number (ENET 1 to ENET 4).
3. Use the arrow keys to highlight the **STATE** field for the interface connector.
4. Use the SPACE bar to step to the appropriate security level (Secure or NonSecure).
5. Use the arrow keys to highlight the **Lock/Learn** field for the interface connector.
6. Use the SPACE bar to step to the appropriate type of security (LockOnNext or LockedOnAddr).
7. If the security level chosen causes the **DisablePort** and **SendTrap** fields to display under Action On Intruder, use the arrow keys to highlight the **DisablePort** field.

If the security level chosen does not cause the fields to display under Action On Intruder, proceed to step 11.

8. To change the **DisablePort** setting to **NoDisable**, press the SPACE bar to toggle the setting.
9. Use the arrow keys to highlight the **SendTrap** field.
10. To change the setting to **NoTrap**, press the SPACE bar to toggle the setting.
11. If the security state selected is LockedOnAddr, use the arrow keys to highlight the **Secure Address** field for the port. Otherwise go to step 13.
12. Enter the address to lock on.

13. To change the security on more than one connector, repeat steps 1 through 11 for each connector. Then proceed to step 14 to save all settings at once.
14. Use the arrow keys to highlight the **SAVE** command.
15. Press ENTER. The message “SAVED OK” displays and all ports of the connector are set to the selected operating mode.

5.21 DEVICE STATISTICS MENU SCREEN

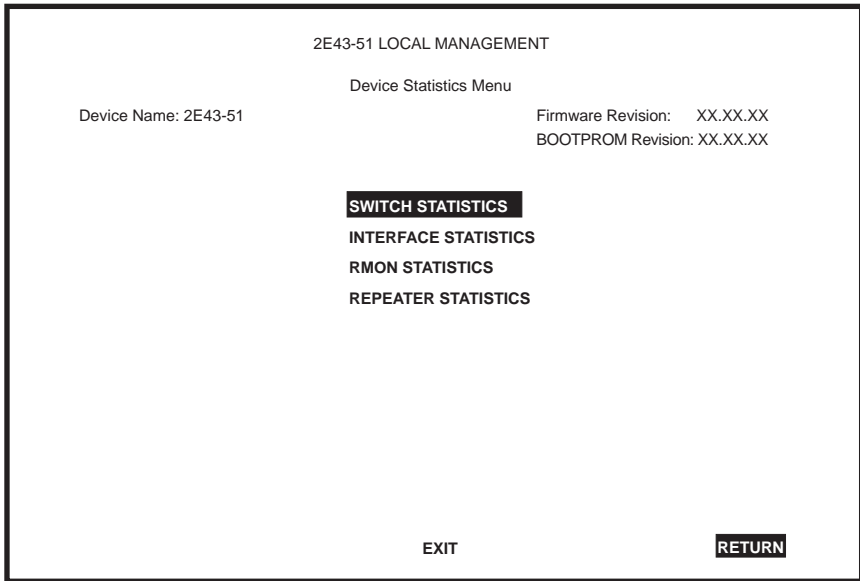
The Device Statistics Menu screen, [Figure 5-28](#), provides access to screens that allow the user to obtain switch statistics about frame traffic through each interface and view operating statistics about each port.



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

[Section 5.7.9](#) provides instructions on setting the operational mode.

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.



22512-67

Figure 5-28 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. For details, refer to [Section 5.22](#).

INTERFACE STATISTICS

The Interface Statistics screen provides the MIB-II statistics for each switched interface, on an interface-by-interface basis. For details, refer to [Section 5.23](#).

RMON STATISTICS

The RMON Statistics screen displays all the statistics gathered by the embedded RMON agent built-in to the 2E43-51. For details, refer to [Section 5.24](#).

REPEATER STATISTICS

The Repeater Statistics screen provides the operating statistics for each port (1 through 48) and its corresponding network (ENETs 1 through 4). For details, refer to [Section 5.25](#).

5.22 SWITCH STATISTICS SCREEN

The Switch Statistics screen, [Figure 5-29](#), lists the number of frames received, transmitted, filtered, and forwarded by each port.

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.

Event Message Line				
2E43-51 LOCAL MANAGEMENT				
Switch Statistics				
Device Name: 2E43-51		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
CLEAR COUNTERS		EXIT		RETURN

22512-26

Figure 5-29 Switch Statistics Screen

The Switch Statistics screen displays the following fields:

Port # (Read-Only)

Identifies the network port. [Table 5-6](#) shows the port organization.

Table 5-6 Port Organization

ENET 1 = Network Port 1, 10 Mbps	Fast Ethernet Slot 5 = Port 5
ENET 2 = Network Port 2, 10 Mbps	Fast Ethernet Slot 6 = Port 6
ENET 3 = Network Port 3, 10 Mbps	HSIM Slot = Port 7
ENET 4 = Network Port 4, 10 Mbps	

Frames Rcvd (Read-Only)

Displays the number of frames received by the port since last power-up or reset.

Frames Txmtd (Read-Only)

Displays the number of frames transmitted by the port since last power-up or reset.

Frames Fltrd (Read-Only)

Displays the number of frames filtered by the port since 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.

5.23 INTERFACE STATISTICS SCREEN

The Interface Statistics screen, [Figure 5-30](#), is used to gather MIB-II statistics for all of the 2E43-51 interfaces (ENET 1 – ENET 4, and Fast Ethernet Interface Modules) with the exception of an installed HSIM.



Cabletron Systems HSIMs gather their own statistics, and may be viewed via the Local Management screens of the applicable HSIM. Refer to your HSIM documentation for information on how to access these screens.

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 displays.

```

Event Message Line
                                2E43-51 LOCAL MANAGEMENT

                                Interface Statistics

Device Name: 2E43-51                Firmware Revision:  XX.XX.XX
                                      BOOTPROM Revision: XX.XX.XX

Interface: 1                        Name: Ethernet Frontpanel

InOctets:          7500456           Address:           00-00-00-00-00-00
InUnicast:         6789              Last Change:      xx days 00:00:00
InNonUnicast:     0                  Admin Status:     Up
InDiscards:       0                  Oper Status:      Down
InErrors:         0
InUnknownProtos: 0                  MTU:              1514
OutOctets:        0                  Speed:            100000000
OutUnicast:       0
OutNonUnicast:    0
OutDiscards:      0                  Link Status:      No Link
OutErrors:        0                  Duplex Mode:      Standard
OutQLen:          0

Interface: [nn]      CLEAR COUNTERS      EXIT      RETURN
  
```

2251_64

Figure 5-30 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 5-30](#) shows the Interface field displaying 1. This represents ENET 1 of the module. To view other interface statistics, refer to [Section 5.23.1](#).

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 including bad frames, and framing characters.

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 it was in an initialization phase and not ready to forward packets, 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.

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 total number of packets that can be held in 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 displays either **Link** or **No Link**.

Duplex Mode (Read-Only)

This field indicates whether the interface is operating in normal (standard) or full duplex mode. This field displays either **Standard** or **Full Duplex**.

Interface [nn] (Command)

This command is used to enter an interface number for viewing statistics. For instructions on how to use this command, refer to [Section 5.23.1](#).

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 5.23.2](#).

5.23.1 Displaying Interface Statistics

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

1. Use the arrow keys to highlight the **Interface [nn]** 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.

Press ENTER (neither the **Interface #** fields nor the statistics will change until ENTER is pressed).

5.23.2 Using the Clear Counters Command

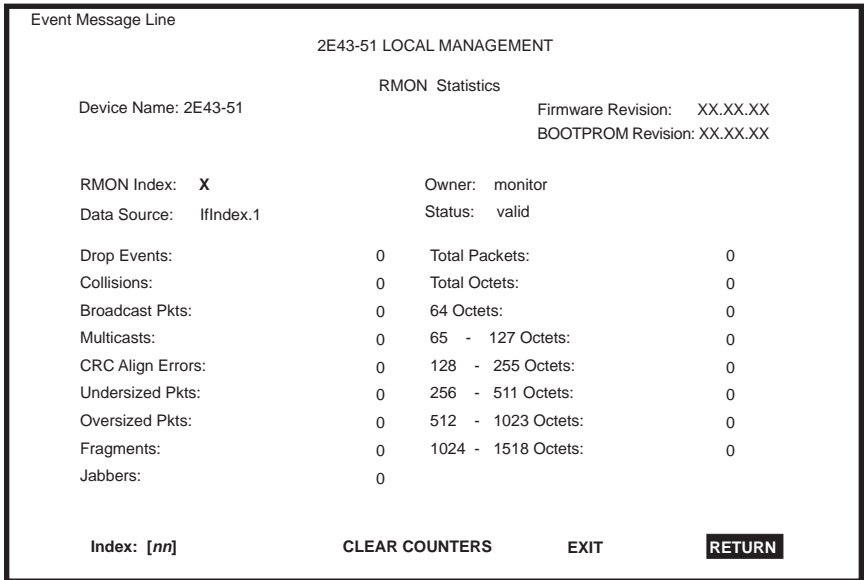
To reset all the statistics counters of the selected interface to zero, perform the following steps:

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

5.24 RMON STATISTICS SCREEN

RMON statistics for each interface, on an interface-by-interface basis, are viewed through the RMON Statistics screen shown in [Figure 5-31](#).

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.



2251_65

Figure 5-31 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 2E43-51 has an embedded RMON agent that gathers statistics for each interface on the module.

Data Source (Read-only)

This field displays the source of the statistics data that is currently being displayed on the screen. Figure 5-31 shows that the data source for this RMON index is Interface 1 (ENET 1) by displaying the name IfIndex.1. If the screen was displaying RMON statistics for Interface 4 (ENET 4), the name displayed would be IfIndex.4.

Owner (Read-only)

This field displays the name of the entity that configured this entry.

Status (Read-only)

The Status field displays the current operating status of the displayed interface. This field will display “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.

Multicasts (Read-only)

The Multicast Pkts 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.

Undersized Pkts (Read-only)

The Undersized Pkts field displays the number of packets received whose size was less than the minimum Ethernet frame size of 64 bytes, not including preamble, but have a valid CRC.

Oversized Pkts (Read-only)

The Oversized Pkts field displays the number of packets received whose size exceeded 1518 data bytes, not including preamble, but have a valid CRC.

Fragments (Read-only)

This field displays the number of received packets that are not the minimum number of bytes in length or received packets that had a bad Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes), and have 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 5.24.1](#).

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 5.24.2](#).

5.24.1 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).

5.24.2 Using the Clear Counters Command

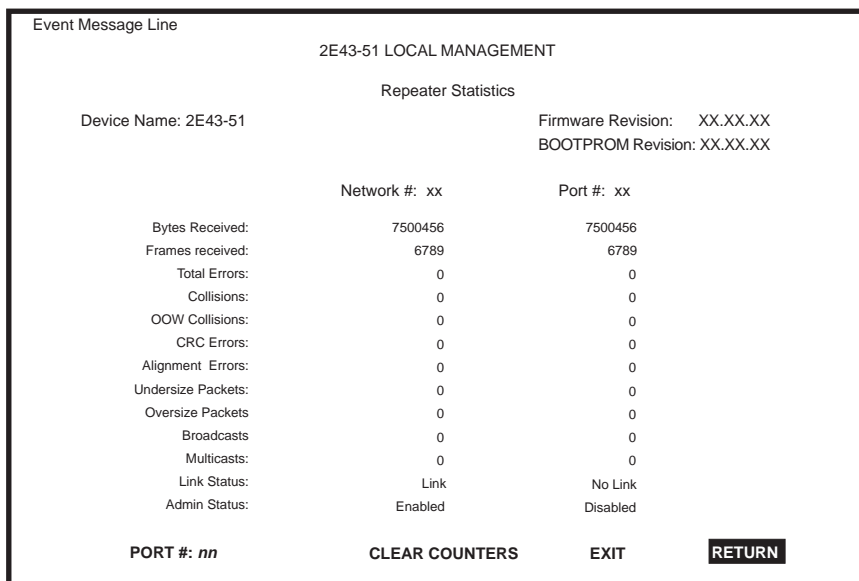
To reset all the statistics counters of the selected interface to zero, perform the following steps:

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

5.25 REPEATER STATISTICS SCREEN

Operating statistics for each repeater port (1 through 48) and its corresponding network (ENETs 1 through 4) are displayed via the Repeater Statistics screen shown in [Figure 5-32](#).

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



22511-29

Figure 5-32 Repeater Statistics Screen for Repeater Ports (1 – 48)

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

Network # (Read-Only)

Indicates the current Ethernet Segment (ENET 1 through ENET 4) port for which statistics are displayed. This field is automatically set by selecting a port number in the PORT # command field at the bottom of the screen. For example, if 14 is selected in the PORT # command field, the statistics for Network 2 (ENET 2) displays along with the statistics for the selected port. If 46 is selected, the statistics for Network 4 (ENET 4) and port 46 displays.

Port # (Read-Only)

Indicates the current port for which statistics are displayed. The port number can be changed by using the PORT # command field at the bottom of the screen. Depending on the port number entered, the Network # field will automatically change to indicate the associated ENET. For details on how to use this field, refer to [Section 5.25.1](#).

Bytes Received (Read-only)

Displays the number of bytes received.

Frames Received (Read-only)

Displays the number of frames received.

Total Errors (Read-only)

Displays the total number of errors.

Collisions (Read-only)

Displays the total number of collisions that were detected.

OOW Collisions (Read-only)

Displays the number of Out Of Window (OOW) collision errors detected. These collisions can be caused by a station on the network violating Carrier Sense and transmitting at will, a cable failure occurring during the transmission of a packet, or a network propagation delay greater than 51.2 μ s.

CRC Errors (Read-only)

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 that is received is the same as the data that was originally sent.

Alignment Errors (Read-only)

Displays the number of alignment errors detected. Alignment errors occur when the total number of bits in the packet are not divisible by eight due to missing bits in the bytes contained in the packet.

Undersize Packets (Read-only)

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 the preamble).

Oversize Packets (Read-only)

Displays the number of packets received with a valid CRC and whose size exceeded 1518 data bytes (not including preamble).

Broadcasts (Read-only)

Displays the number of broadcasts transmitted and received.

Multicasts (Read-only)

Displays the number of multicasts transmitted and received.

Link Status (Read-only)

Indicates if the network or port is linked (**Link**) or not linked (**No Link**).

Admin Status (Read-only)

Indicates if the network or port is enabled (**Enabled**) or disabled (**Disabled**).

PORT # (Command)

This command is used to select a port to view its statistics and those of its associated Network. For details, refer to [Section 5.25.1](#).

CLEAR COUNTERS (Command)

This command sets all statistics counters to zero. For details on how to use this command, refer to [Section 5.25.2](#).

5.25.1 Displaying Repeater Statistics

To display the statistics for any repeater port (1 – 48), proceed as follows:

1. Use the arrow keys to highlight the **Port #** command field at the bottom of the screen.
2. Press the SPACE bar to increment or press the BACKSPACE key to decrement the port number.
3. Press ENTER (the Port #, the Network #, and the statistics do not change until ENTER is pressed).

5.25.2 Using the Clear Counters Command

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

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command field at the bottom of the screen.
2. Press ENTER, the counters for the selected port are reset to zero.

5.26 NETWORK TOOLS

The Network Tools function allows the user to access and manage network devices. Figure 5-33 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.

```
Welcome to Network Tools

-> help

Commands Available to User

Built in Commands:

arp          bridge      defroute
netstat      ping        reset
show         traceroute

soft_reset   telnet      link_trap

atm_stp_state

SPECIAL:
done, quit, or exit - Exit from the Network Tools.
For help with a specific command, type 'help <command>'.

->
```

090829

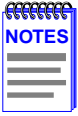
Figure 5-33 Network Tools Screen

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 the user to access and manage network devices. The commands are **arp**, **bridge**, **defroute**, **netstat**, **ping**, **reset**, **show**, **traceroute**, **soft-reset**, **telnet**, **link_trap**, and **atm_stp_state**.

- Special Commands – Allow the user to exit from Network Tools. The commands are **done**, **exit**, and **quit**.



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 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.

5.26.1 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
# (30)          122.144.40.111    00.00.0e.12.3c.04  3(dynamic)
# (30)          122.144.48.109    00.00.0e.f3.3d.14  3(dynamic)
# (30)          122.144.52.68     00.00.0e.12.3c.04  3(dynamic)
# (30)          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 allows bridge management to be enabled or disabled at the user's 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: Not Applicable

Example:

```
-> bridge disable all  
  
-> bridge enable 1  
  
-> bridge disable 1
```

05141-68

defroute:

Syntax: defroute
defroute [interface number] [IP address]

defroute delete [interface number] [IP address]

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

Options: Not Applicable

Example:

```
-> defroute 2 147.152.42.32
```

05141-69

netstat:**Syntax:** netstat [option]**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:** Not Applicable**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 the user configuration settings from NVRAM. The user 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:

```
-> 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: Not Applicable

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: Not Applicable

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 the user configuration settings from NVRAM. The user 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 the user to communicate with another host (that supports Telnet connections) using the Telnet protocol. The user 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: Not Applicable

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
LINK TRAP STATUS:
    Port 1 is ENABLED      Port 2 is DISABLED
    Port 3 is ENABLED      Port 4 is ENABLED

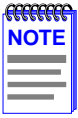
-> link_trap disable 2
Link traps have been DISABLED on port 2

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

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

2314-78

atm_stp_state:



The **atm_stp_state** command is only available if an HSIM-A6DP is installed in the device (e.g., 2E43-51). This command allows the user to enable, disable, or check the current status of the Spanning Tree Algorithm on all ATM interfaces.

Syntax: atm_stp_state [STATE]

Description: The atm_stp_state command allows the user to enable, disable, or check the status of the Spanning Tree Algorithm on all ATM interfaces. The user must specify the STATE option as enable, disable, or status. The STATE field is mandatory.

Options: enable, disable, status

Example:

```
-> atm_stp_state status
Atm Stp is Enabled
-> atm_stp_state disable
-> atm_stp_state enable
```

2314-79

5.26.2 Special Commands

done, quit, exit:

Syntax: done, quit, or exit

Description: The done, quit, or exit command enables the user 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 2E43-51 and 2E43-51R. 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):	20 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) 2E43-51:	3.15 kg (7 lb)
Weight (Unit) 2E43-51R:	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

- ENET 1 through ENET 4 (ports 1 through 4): Ethernet (10BASE-T compliant) with RJ21 type connectors. Each connector provides connection for 12 twisted pair ports.
- Slots for optional Fast Ethernet Interface Modules (ports 5 and 6): Slots accept three types of optional Fast Ethernet Interface Modules: FE100-TX, FE100-FX, and FE100-F3.
- Slot for optional HSIM: Slot accepts optional High Speed Interface Modules.

A.6 COM 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, AS/NZS 3548, VCCI V-3, and 89/336/EEC.

APPENDIX B

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

The 2E43-51 supports three Fast Ethernet Interface Modules:

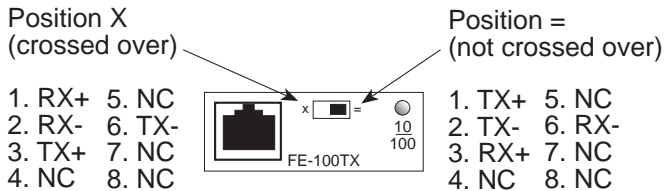
- FE-100TX (Section B.1)
- FE-100FX (Section B.2)
- FE-100F3 (Section B.3)

This appendix provides the specifications for these modules.

B.1 FE-100TX

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

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.



16651_05

Figure B-1 FE-100TX RJ45 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.

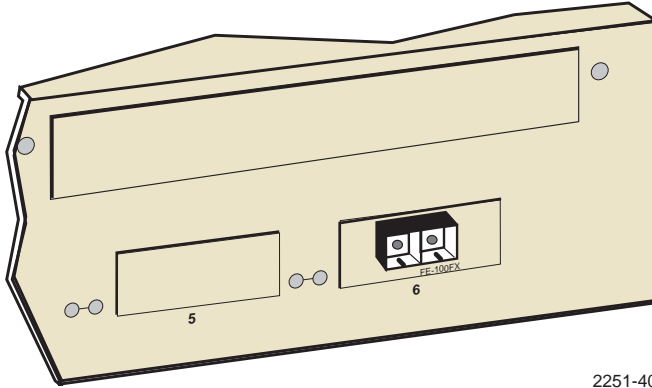
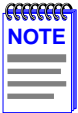


Figure B-2 FE-100FX

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



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.

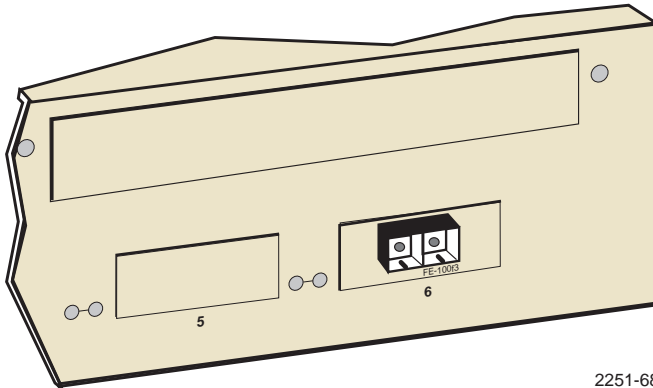


Figure B-3 FE-100F3

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



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 PERSONNALL 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 and the High Speed Interface Module.

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 2E43-51 chassis cover.



DO NOT REMOVE THE COVER FROM THE 2E43-51 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 2E43-51 AGAIN UNTIL THE COVER AND SCREWS ARE IN PLACE.

DECKEL VON DAS 2E43-51 NICHT ABZIEHEN UNTER SPANNUNG. GEFAHR FÜR DAS PERSONNAL UND/ODER DAS GERÄT WEGEN GEFÄHRLICHE SPANNUNGEN ENSTEHT.

2E43-51 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:

1. Disconnect the 2E43-51 from the network as follows:
 - a. For the 2E43-51, unplug the power cord from the rear of the chassis. For the 2E43-51R, unplug both power cords from the rear of the chassis.



TURN OFF THE 2E43-51 BY UNPLUGGING THE POWER CORD FROM THE REAR OF THE CHASSIS.

AM HINTEN DES 2E43-51 STECHEI ABZIEHEN UM AUS ZU SCHALTEN.

APAGUE EL 2E43-51 DESENCHUFE EL CABLE DE LA UNIDAD.

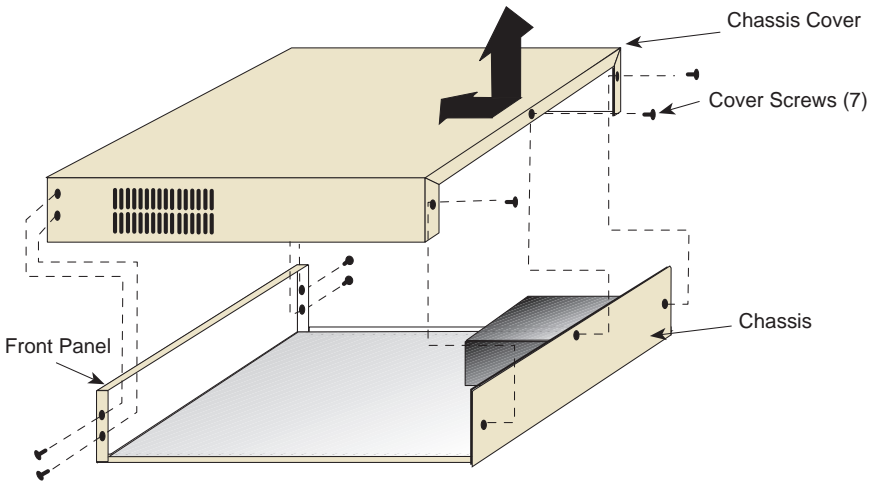


Before performing step b, mark the cables connected to the 2E43-51 according to their associated port numbers. This is recommended for ease of reinstallation.

- b. Disconnect all network cables attached to the 2E43-51.

2. If the 2E43-51 is rack mounted, remove it from the rack and remove the rackmount brackets (refer to **Chapter 3, Optional Installations and Mode Switch Bank Settings**).
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 of 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.

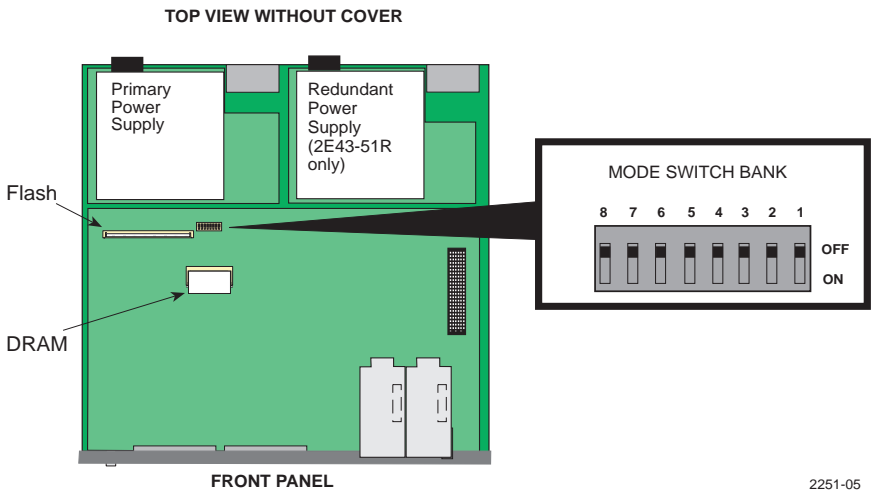
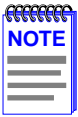


Figure C-2 2E43-51 Mode Switch Location/Component Layout

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. Do NOT attempt a Forced BootP unless a BootP server has been configured for the 2E43-51. The BootP server references the location of a station acting as a Trivial File Transfer Protocol (TFTP) server containing the 2E43-51 image file. When the position of Switch 6 is changed and the power is cycled to the 2E43-51, 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 2E43-51 will continue to request either the BootP server or the TFTP server until the RESET button on the 2E43-51 is pressed. Once the RESET button is pressed, the 2E43-51 will reset after one minute and load the image stored in FLASH memory.

- **Switch 7** – Clear NVRAM. Changing the position of this switch resets NVRAM on the next power-up. All user-entered parameters, such as the IP address, device names, etc., are reset to the factory default settings. Once the 2E43-51 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 the next power-up. Once the 2E43-51 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 module 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 on for ports 5 and 6 and the High Speed Interface Module for port 7.

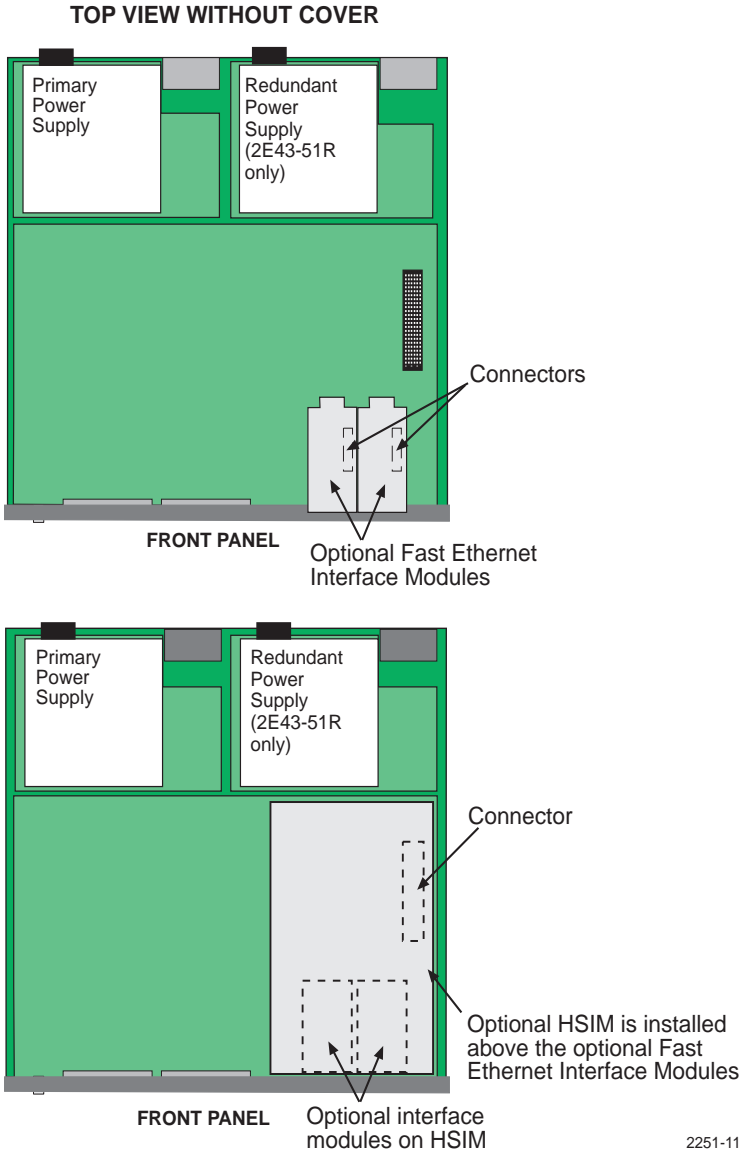
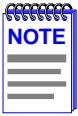


Figure C-3 Fast Ethernet Interface Module Connector Location



The installation instructions for the High Speed Interface Modules are in the associated user's guide.

To install a Fast Ethernet Interface Module in port slot 5 or 6, proceed as follows:



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.

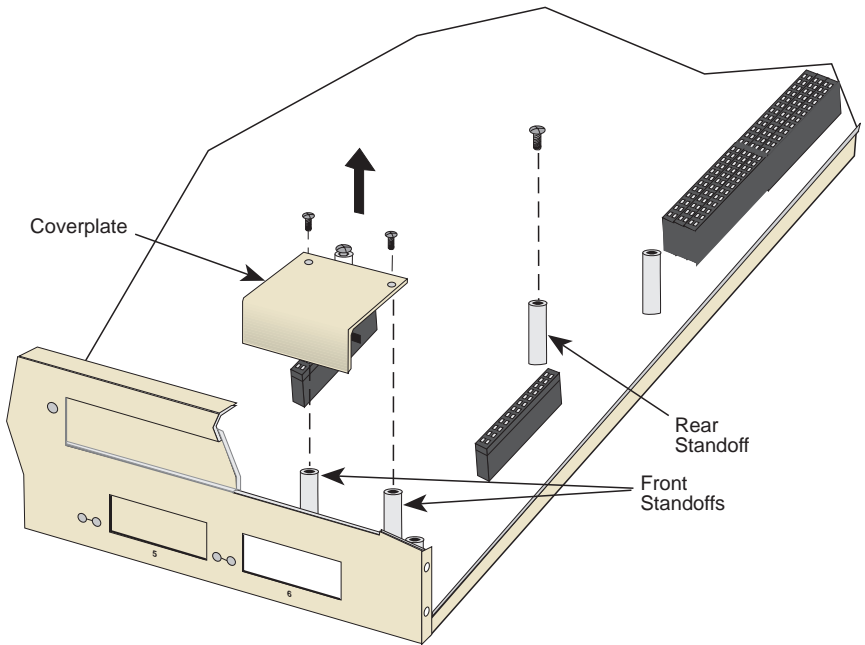


The Fast Ethernet Interface Module and the 2E43-51 are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could damage the module or the 2E43-51.



When installing Fast Ethernet Interface Modules in both port slots 5 and 6, remove the coverplates from both slot openings. In the following instructions, the optional module is shown being installed in port slot 6.

1. Remove the coverplate from the port slot where the Fast Ethernet Interface Module will 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.



2251-38

Figure C-4 Coverplate Removal

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



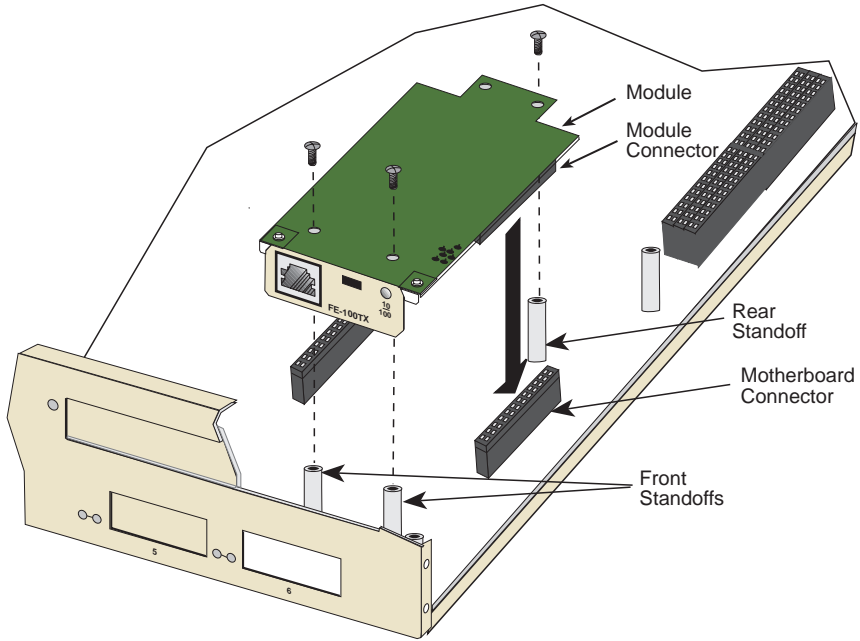
When installing an FE-100FX or FE-100F3 module into the 2E43-51, remove the rubber plug on the module before proceeding.

3. See [Figure C-5](#). Gently pull the faceplate of the 2E43-51 forward to allow room for the Fast Ethernet Interface Modules to be aligned over the connector.



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.

- Carefully lower the Fast Ethernet Interface Module onto the standoffs while inserting the module connector into the associated Motherboard Connector.



2251-39

Figure C-5 Installing the Fast Ethernet Interface Module

- 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.
- Secure the Fast Ethernet Interface Module with the screws saved in steps 1 and 2.
- Reinstall the cover.

INDEX

Numerics

- 100BASE-FX
 - single mode cable length 2-2
- 10BASE-T
 - connection 3-9
 - requirements 2-1
- 2E43-51
 - front panel 1-3

A

- Access policy 5-32
- Auto-Negotiation 1-4

B

- Bridge Configuration screen
 - state 5-37
- Broadcast Suppression screen 5-58
 - peak rate 5-59
 - port # 5-59
 - reset peak 5-60
 - threshold 5-60
 - time since peak 5-59
 - total RX 5-59
- Built-in Commands
 - use of 5-85

C

- Cable specifications
 - 100BASE-FX MMF 2-2
 - 100BASE-T network 2-1
 - 100BASE-TX network 2-2
- Chassis cover, removal of C-2
- CLEAR 5-83
- COM port 5-27
 - pin assignments A-2
- Command Set 5-85
- Connecting to the network 3-9
- Crossover switch B-1

D

- Default gateway 5-18, 5-22
- Device Configuration screen 5-15
- Device date 5-18
- Device Menu screen 5-13
- Device Specific Configuration Menu screen 5-39
- Device Statistics Menu screen 5-69
- Device time 5-18
- Document conventions 1-8

E

- Environmental requirements A-2

F

- FE-100F3
 - transmitter specifications B-3
- FE-100FX
 - transmitter specifications B-2
- FE-100TX
 - RJ45 Pinouts B-1
- Fiber connection
 - SC to SC 3-14
- Flash Download screen 5-50
 - download file name 5-53
 - download method 5-52
 - download serverIP 5-53
 - last image file name 5-52
 - last image serverIP 5-52
 - reboot after download 5-52
 - TFTP gateway IP addr 5-52

G

- General Configuration screen 5-17
 - application 5-20
 - COM port 5-27
 - default gateway 5-18, 5-22
 - device date 5-18

- device time 5-18, 5-24
- IP address 5-18, 5-20
- MAC address 5-17
- Operational Mode 5-26
- screen lockout time 5-19, 5-25
- screen refresh time 5-18, 5-25
- subnet mask 5-18, 5-21

Getting help 1-9

H

- High Speed Configuration Interface
 - screen 5-46
- High Speed Interface Configuration
 - Menu screen 5-44
- High Speed Interface screen
 - advertised ability 5-48
 - configuring an FE-100FX 5-48
 - configuring an FE-100TX 5-49
 - current operational mode 5-47
 - desired operational mode 5-47
 - link status 5-47
 - port type 5-47
 - setting the FE-100FX 5-49
 - setting the FE-100TX 5-49

I

- Installation
 - connecting to the network 3-9
 - Fast Ethernet Interface Module C-7
- Interface Statistics Screen
 - address 5-75
 - admin status 5-75
 - CLEAR COUNTERS 5-76
 - duplex mode 5-76
 - InDiscards 5-74
 - InErrors 5-74
 - InNonUnicast 5-74
 - InOctets 5-74
 - interface 5-74, 5-76
 - InUnicast 5-74
 - InUnknownProtos 5-74
 - last change 5-75
 - link status 5-76

- MTU 5-76
- name 5-74
- oper status 5-75
- OutDiscards 5-75
- OutErrors 5-75
- OutNonUnicast 5-75
- OutOctets 5-75
- OutQLen 5-75
- OutUnicast 5-75
- speed 5-76
- IP address 5-18, 5-20
- IP Fragmentation 5-20
 - enabling/disabling of 5-30

K

- Keyboard conventions 5-2

L

- LANVIEW LEDs 4-1
- Local Management
 - exiting from 5-11
 - introduction to 1-6
 - Password screen 5-8
- Local Management screens
 - selection of 5-11

M

- Management
 - use of 1-6
- Management Terminal
 - COM port connection of 5-3, 5-4
 - setup of 5-3, 5-5
- Mode Switch
 - setting C-4

N

- Port Redirect Function screen
 - destination port 5-57
 - source port 5-57
- Network connection
 - FE-100FX/FE-100F3 3-14
 - FX-100TX 3-11
- Network Connections 3-9

- Network Tools
 - built-in commands 5-85
 - arp 5-86
 - atm_stp_state 5-94
 - bridge 5-88
 - defroute 5-88
 - netstat 5-89
 - ping 5-89
 - reset 5-90
 - show 5-90
 - traceroute 5-91
 - description of 5-85
 - special commands 5-86
 - done 5-94
 - exit 5-94
 - quit 5-94
- Network Tools commands
 - traceroute 5-94
- Network Tools screen
 - accessing of 5-85
- NVRAM
 - clearing of 5-29
- O**
- Operational Mode 5-26
- P**
- Password screen 5-8
- Passwords 5-31
- Physical properties A-1
- Port Level Security Configuration
 - screen
 - action on intruder 5-67
 - interface # 5-68
 - lock/learn 5-67
 - port 5-66
 - secure address 5-67
 - state 5-66
- Port Level Security Configuration
 - screen
 - 5-65
- Port Redirect Function screen
 - destination port 5-56
 - errors 5-57
 - remap errors 5-56
 - source port 5-56
 - status 5-57
- R**
- Regulatory Compliance A-3
- Related manuals 1-10
- Repeater Configuration Menu
 - screen 5-61
- Repeater Level Security
 - Configuration screen 5-62
 - action on intruder 5-64
 - interface 5-63
 - lock/learn 5-63
 - state 5-63
- Repeater Statistics screen
 - administration status 5-83
 - alignment errors 5-83
 - broadcasts transmitted/
 - received 5-83
 - bytes received 5-82
 - CLEAR COUNTERS 5-83
 - collisions 5-82
 - CRC errors 5-82
 - frames received 5-82
 - link status 5-83
 - multicasts transmitted/
 - received 5-83
 - network 5-82
 - OOW collisions 5-82
 - oversize packets 5-83
 - PORT# 5-83
 - port# 5-82
 - total errors 5-82
 - undersize packets 5-83
- RESET button 4-7
- RMON Statistics screen
 - 1024 – 1518 octets 5-80
 - 128 – 255 octets 5-80
 - 256 – 511 octets 5-80
 - 512 – 1023 octets 5-80
 - 64 octets 5-79
 - 65 – 127 5-80
 - 65 – 127 octets 5-80

- broadcast pkts 5-78
- CLEAR COUNTERS 5-80
- collisions 5-78
- CRC align errors 5-78
- data source 5-78
- drop events 5-78
- fragments 5-79
- index 5-80
- jabbers 5-79
- multicasts 5-78
- oversize packets 5-79
- owner 5-78
- RMON index 5-77
- status 5-78
- total octets 5-79
- total packets 5-79
- undersize packets 5-79
- Runtime IP address discovery 1-5

S

- Safety information
 - laser iv
- Screen lockout time 5-25
- Screen refresh time 5-25
- Screens
 - Broadcast Suppression screen 5-58
 - Device Configuration screen 5-15
 - Device Menu screen 5-13
 - Device Specific Configuration
 - Menu screen 5-39
 - Device Statistics Menu screen 5-69
 - exiting from 5-11
 - FLASH Download screen 5-50
 - General Configuration screen 5-17
 - hierarchy of 5-9
 - High Speed Interface Configuration
 - Menu screen 5-44
 - High Speed Interface Configuration screen 5-46
 - Interface Statistics screen 5-73
 - Network Tools screen 5-85
 - Password screen 5-8
 - Port Level Security Configuration screen 5-65
 - Port Redirect Function screen 5-55
 - Repeater Configuration Menu screen 5-61
 - Repeater Level Security
 - Configuration screen 5-62
 - Repeater Statistics screen 5-81
 - RMON Statistics screen 5-77
 - selection of 5-11
 - SNMP Community Names
 - screen 5-31
 - SNMP Traps screen 5-34
 - Switch Configuration screen 5-36
 - Switch Statistics screen 5-71
 - System Resources screen 5-41
- Security
 - setting of port level security 5-68
 - setting of repeater level security 5-64
- Setup of
 - management terminal 5-5
- SNMP Community Names
 - setting of 5-31
- SNMP Community Names screen
 - access policy 5-32
 - community name 5-32
- SNMP Traps screen 5-34
 - enable traps 5-35
 - trap community name 5-34
 - trap destination 5-34
 - trap table configuration 5-35
- Spanning Tree Algorithm 5-37
- Special Commands
 - use of 5-86
- Special Commands, Network Tools 5-94
- Specifications A-1
- Standards compatibility 1-6
- Subnet mask 5-18, 5-21
- Switch address 5-37
- Switch Configuration screen 5-36
 - age time 5-38
 - MAC address 5-37
 - number of ports 5-37
 - port # 5-37

- port status 5-39
- selecting the STA 5-38
- status 5-38
- switch address 5-37
- type of STA 5-37

Switch Statistics screen 5-71

- clearing counters 5-72
- frames fltrd 5-72
- frames frwded 5-72
- frames rcvd 5-72
- frames txmtd 5-72
- interface # 5-72

System Resources screen

- CPU type 5-42
- current switch utilization 5-43
- DRAM installed 5-42
- FLASH memory installed 5-42
- NVRAM installed 5-43
- peak switch utilization 5-43
- reset peak switch utilization 5-43

T

- Telnet connections 5-6
- TFTP gateway Ip addr 5-52
- Trap table configuration 5-35
- Traps
 - enable 5-35
- Troubleshooting 4-1
 - checklist 4-6

U

- Uninterruptible Power Supply
 - COM configuration for 5-7
 - connection of 5-7
- Unpacking 3-2

V

- VLAN
 - configuration of 5-41

