EMM-E6

USER'S

GUIDE

EMM-E6

SN

RESET ○

CPU ○

D C B A

STBY ○ ○ ○ ○
RCV ○ ○ ○ ○
XMT ○ ○ ○ ○
CLN ○ ○ ○ ○

BRIM-F6

STY XMT
LNK RCV

E

PWR

EPIM-A

E
P
I
M
1

PWR

EPIM-A

E
P
I
M
2

C
O
M
1

C
O
M
2

F

ETHERNET

CABLETRON
SYSTEMS
The Complete Networking Solution™

CABLETRON SYSTEMS, P.O. Box 5005, Rochester, NH 83866-5005

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.

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.

DOC 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 equipment is in the Class I Category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI) aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers, etc.

Read the instructions for correct handling.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。

取扱説明書に従って正しい取り扱いをして下さい。

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. <u>LICENSE.</u>   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. <u>OTHER RESTRICTIONS.</u>   You may not reverse engineer, decompile, or disassemble the Program.

3. <u>APPLICABLE LAW.</u>   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.

BELLCORE TESTING INFORMATION

This product has been tested by Bellcore and found to comply with the following Bellcore Standards:

1. TR-NWT-000063: Network Equipment Building System (NEBS) Generic Equipment Requirements

2. GR-1089-CORE: EMC and Electrical Safety Generic Criteria for Network Telecommunications Equipment.

EXCLUSION OF WARRANTY AND
DISCLAIMER OF LIABILITY

1. <u>EXCLUSION OF WARRANTY.</u>   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 EXPRESS 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. <u>NO LIABILITY FOR CONSEQUENTIAL DAMAGES</u>.   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 WARRANTEES, 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.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

APPENDIX A   EMM-E6 SPECIFICATIONS

APPENDIX B   EMM-E6 OIDs

CHAPTER 1

INTRODUCTION

Welcome to the Cabletron Systems **EMM-E6 User's Guide**. This manual explains how to set-up, configure, and locally manage the Cabletron Systems 6-port Ethernet Bridge/Management Module (EMM-E6).

1.1   USING THIS MANUAL

Read through this manual completely to familiarize yourself with its content and to gain an understanding of the features and capabilities of the EMM-E6 and its Local Management, or LM, functions. A general working knowledge of Ethernet and IEEE 802.3 type data communications networks and their physical layer components is helpful when installing the EMM-E6 module and when using LM.

Chapter 1, **Introduction**, outlines the contents of this manual, briefly describes the EMM-E6's features, provides a brief review of IP addressing, and concludes with a list of related manuals.

Chapter 2, **Requirements/Configurations**, explains the network requirements to consider before installing the EMM-E6. This chapter also includes sample configurations to demonstrate various applications for the EMM-E6.

Chapter 3, **Installation**, provides instructions/guidelines on how to install the EMM-E6 into an MMAC-FNB, set the EMM-E6 mode switches, and connect segments to your device using optional EPIMs. This chapter also explains how to install optional Single In-line Memory Modules, EPIMs, and locate Bridge Router Interface Module (BRIM) connectors.

Chapter 4, **Attaching a Console**, describes how to attach a Local Management console to the EMM-E6. This chapter provides the setup and configuration requirements for the console, the console cable, and any cable connections.

Chapter 5, **Accessing Local Management**, describes how to access LM after you attach the management console.

Chapter 6, **Community Names**, explains how to use the Community Name Table screen to set both local and remote access levels.

Chapter 7, **Configuration Screen**, describes how to assign IP addresses, subnet masks, and the default gateway to the EMM-E6. This chapter also explains how to enable and disable all ports.

Chapter 8, **Trap Table Screen**, explains how to designate management stations as recipients of SNMP alarm or event traps.

Chapter 9, **SNMP Tools Screen**, provides information on the resident EMM-E6 Management Information Base (MIB) walking tool.

Chapter 10, **Router Setup Screen**, Shows the Routing Services Setup Screen, where the EMM-E6's optional Routing Services may be accessed.

Chapter 11, **Device Statistics Screen**, illustrates the statistics provided by EMM-E6/LM. This chapter also describes how to enable and disable specific ports on the EMM-E6, and set the statistics update frequency time.

Chapter 12, **Command Line Interface Screen**, shows the Command Line Interface (CLI) screen. This screen will function in future releases of EMM-E6 firmware.

Chapter 13, **MIB Navigator**, provides instructions and examples for using the navigator command set.

Chapter 14, **Troubleshooting**, details the EMM-E6 LANVIEW® LEDs that enable you to quickly diagnose network/operational problems and provides suggested courses of action for troubleshooting.

Chapter 15, **Image File Download**, provides instructions to download a new image file to the EMM-E6 by setting specific MIB OID strings.

Appendix A, **EMM-E6 Specifications**, details the properties of the EMM-E6 and currently available EPIM modules.

Appendix B, **OID Descriptions**, supplies information detailing the Object Identifiers that may be accessed for managing the EMM-E6.

Following the Appendices is a brief **Glossary of Terms** which provides short definitions for terms related to items and concepts referred to in this manual.

1.2 EMM-E6 FEATURES

- i960 Processor Design

- IEEE 802.1d Compliant

- Available Routing Services

- Special Filtering Database

- Six port Ethernet Bridge

- Integrated BRIM technology

- User Configurable EPIMs

- Expandable Flash EEPROM
  Memory and Runtime download

- Expandable Local DRAM

- Expandable Shared DRAM

- SNMP and RMON Support

- LANVIEW Diagnostic LEDs

- DLM Support

- Local Communication Ports

- UPS Proxy Agent Support

- In-Band Telnet with MIB
  Navigator

- Port Locking and
  LANVIEWSECURE Support
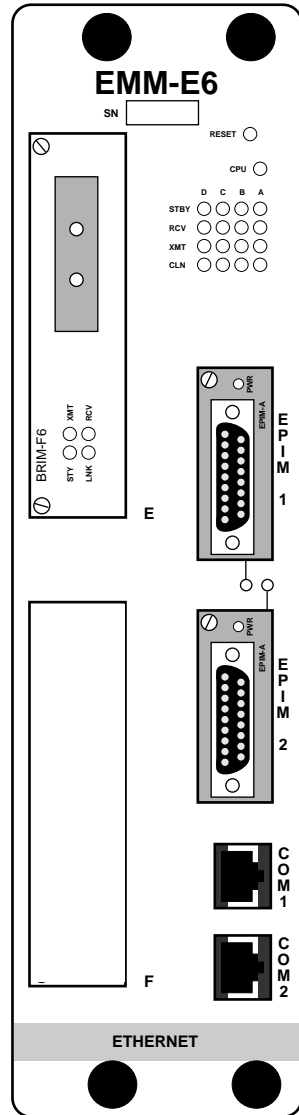
i960 Processor Design

The EMM-E6 is equipped with an advanced Intel i960 microprocessor that provides a scalable RISC-based architecture.

IEEE 802.1d Compliant

The EMM-E6 is a fully IEEE 802.1d compliant Ethernet bridge. The EMM-E6 supports both the IEEE and DEC Spanning Tree algorithms, allowing it to operate in several fault-tolerant bridging environments.

Available Routing Services

Cabletron's own routing services for the EMM-E6 are available as a software upgrade. When properly configured with the software upgrade, the EMM-E6 is capable of routing IP, IPX, DECnet, AppleTalk, and OSPF.

Special Filtering Database

The EMM-E6 supports a special filtering database which allows packets to be blocked from crossing the bridge based on manager-defined parameters.

Six Port Ethernet Bridge

The EMM-E6 has six Ethernet ports. Three of these ports (Ethernet Channels A, B, and C) operate within the hub. One other port (Ethernet Channel D) provides an external connection through one of two Ethernet Port Interface Modules (EPIMs) located on the EMM-E6 faceplate. The remaining two ports (Ethernet Channels E and F) are externally accessible through the use of Cabletron Bridge/Router Interface Modules (BRIMs), which can be configured in the module.

Integrated BRIM Technology

In addition to Ethernet Channels A through D, the EMM-E6 provides management for up to two optional Bridge/Router Interface Modules (BRIMs). These modules allow for additional Ethernet connections or Fiber Distributed Data Interface (FDDI) network backbones. The following lists optional BRIMs:
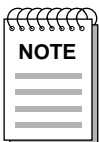
NOTE

For current information on the available BRIM modules supported by the EMM-E6, please refer to the Release Notes shipped with the module or contact Cabletron Systems.

- **BRIM-E6**: Ethernet module with selectable EPIM connection
- **CRBRIM-W/E-IP**: Cisco Router Ethernet/Wide Area module for TCP/IP traffic.
- **CRBRIM-W/E-DESKTOP**: Cisco Router Ethernet/Wide Area module for IP, IPX, DECNet, and AppleTalk traffic.
- **CRBRIM-W/E-ENT**: Cisco Router Ethernet/Wide Area module for all standard Cisco protocols.
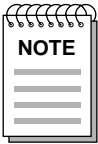
> **NOTE**
>
> *All CRBRIM-W/E products provide two WAN interfaces and one internally connected Ethernet interface. The Ethernet connection is provided through the use of an EPIM-3PS, which is included with the purchase of the CRBRIM-W/E product.*

- **BRIM-F0**: 100 Mbps FDDI Dual Attached Station (DAS) Media Interface Connector (MIC) connection for multimode fiber optic media.
- **BRIM-F5**: 100 Mbps FDDI DAS MIC connection for single mode fiber optic media
- **BRIM-F6**: 100 Mbps FDDI Dual Attach Station connection with configurable connectors

The BRIM-F6 uses FDDI Port Interface Modules (FPIMs). The FPIMs allow a media flexibility for FDDI connections by providing connector and media types meeting several ANSI standards. The following FPIM types are currently available:

- **FPIM- 00**: MultiMode Fiber - Physical Media Dependant (MMF-PMD) compliant multimode fiber optic MIC connector
- **FPIM- 02**: Twisted Pair - Physical Media Dependant (TP-PMD) complaint Unshielded Twisted Pair RJ45 connector
- **FPIM- 04**: TP-PMD compliant Shielded Twisted Pair RJ45 connector.
- **FPIM- 05**: Single Mode Fiber - Physical Media Dependant (SMF-PMD) compliant single mode fiber optic MIC connector.

- **BRIM-A6**: 100/155 Mbps ATM Station connection with configurable connector.

The BRIM-A6 uses ATM Port Interface Modules (APIMs). APIMs allow a media flexibility for ATM connections like that provided by FPIMs (described above). The following APIM types are currently available:

- **APIM-11**: 100 Mbps multimode fiber optic SC connector
- **APIM-21**: 155 Mbps multimode fiber optic SC connector
- **APIM-29**: 155 Mbps single mode fiber optic SC connector

User Configurable EPIMs

The fourth channel (D) directs traffic to one of two external Ethernet Port Interface Modules (EPIMs). The following list contains the currently available EPIMs:

- **EPIM-T**: 10BASE-T RJ45 Port
- **EPIM-F1**: Sub-Miniature Assembly (SMA) connectors for multimode fiber optics
- **EPIM-F2**: Straight-Tip (ST) connectors for multimode fiber optics
- **EPIM-F3**: Straight-Tip (ST) connectors for single mode fiber optics
- **EPIM-C**: RG-58 connector for thin coaxial cabling
- **EPIM-A**: Female DB15 connector for AUI cabling
- **EPIM-X**: Male DB15 connector for AUI cabling

Expandable Flash EEPROM Memory

The EMM-E6 incorporates 2 MB of Flash Electrically Erasable Programmable Read Only Memory (Flash EEPROM). Flash memory holds the operating instruction code of the EMM-E6. When the module is activated, the instruction code (firmware) held in Flash memory is forwarded to Main memory, decompressed, and used to startup the EMM-E6. As the decompression of firmware slightly delays the initialization of the EMM-E6, a Flash memory upgrade is available that allows the firmware to be held in its expanded form.

Flash memory allows for the downloading of firmware to the module without requiring that the module be shut down. The firmware download may be performed at any time during the operation of the module, and the new firmware image will be utilized at the next reset of the module.

Expandable LDRAM
The EMM-E6 comes with 8 MB of Local Dynamic Random Access Memory (LDRAM). LDRAM is the "Main" memory from which the routing or bridging functionality of the EMM-E6 operates. When the EMM-E6 needs to support additional functionality, an LDRAM upgrade may be required. If you are planning to add any functionality to your EMM-E6 module, determine if an LDRAM expansion is required.

Expandable SDRAM
The EMM-E6 comes with 4 Megabytes (MB) of Shared Dynamic Random Access Memory (SDRAM). SDRAM holds packets coming onto the module temporarily while forwarding, filtering, and error checking decisions are made. While SDRAM has been designed to facilitate future expansion, at this time there are no EMM-E6 functions which require or are assisted by the expansion of SDRAM memory.

SNMP and RMON support
Since the EMM-E6 is SNMP compliant, you can control and monitor the device remotely and locally using different SNMP Network Management packages. EMM-E6 firmware also supports several RMON groups, including:

- Alarms
- Events
- History
- Host

- HostTopN
- Matrix
- Statistics

LANVIEW Diagnostic LEDs
Cabletron provides a visual diagnostic and monitoring system, called LANVIEW, with the EMM-E6. LANVIEW LEDs can help you quickly identify device, port, and physical layer problems.

DLM Support
The EMM-E6 allows the option of using Cabletron Distributed LAN Monitor (DLM) software to locally poll and monitor any Simple Network Management Protocol (SNMP) or Internet Protocol (IP) device. The EMM-E6 itself tallies the polling results and can be configured to contact a management station when a predetermined threshold is exceeded. This allows the EMM-E6 to request management attention when it is required, reducing management polling over the network.

Local Communication Ports
The EMM-E6 provides two RJ45 serial ports on its front panel. The COM 1 port allows a serial management connection to an American Power Conversion Smart Uninterruptible Power Supply (UPS). The COM 2 port allows you to access Local Management by locally connecting a DEC VT220 or VT320 terminal, or a PC using VT emulation software.

In-Band Telnet with MIB Navigator
EMM-E6 firmware supports a management tool which allows for MIB navigation from a remote Telnet station.

Port Locking and LANVIEWSECURE Support
The EMM-E6 supports Port Locking features and Cabletron's LANVIEWSECURE line of Media Interface Modules (MIMs). The EMM-E6 is capable of configuring and controlling LANVIEWSECURE MIMs through local or remote management. These security features can help reduce the possibility of network eavesdropping.

1.3   THE MMAC WITH FLEXIBLE NETWORK BUS

The Multi Media Access Center with Flexible Network Bus
(MMAC-FNB) provides the operational platform for the EMM-E6. The
MMAC-FNB (backplane) provides two physically separate buses -
Channel A (operating over the MMAC Power and Management bus), and
Channels B and C (on the FNB). Each of these channels/buses allows
different MIM types to access the EMM-E6 (Figure 1-1).

These channels/buses interconnect through the EMM-E6 to provide
bridging or routing and management for all MIMs in the MMAC chassis.
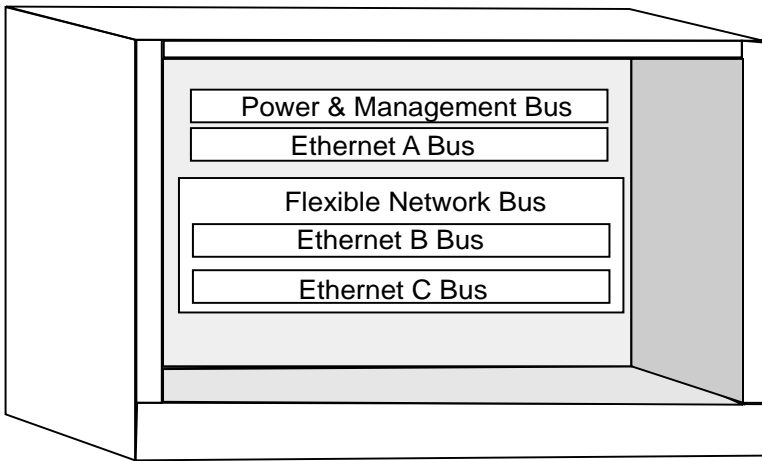
Figure 1-1. MMAC Flexible Network Bus

Two types of MMACs currently support FNB architecture - shunting and
non-shunting. MMACs equipped with shunting backplanes allow
modules operating on Channels B and C to continue communicating with
the EMM-E6, regardless of whether there is an empty slot or an Ethernet
Channel A module between them in the chassis. The following table gives
the part numbers of the MMAC chassis that have shunting capabilities.

Table 1-1. MMACs with Shunting Capabilities

MMAC Chassis	Part #
MMAC-3FNB	**FC**000000000 or above
MMAC-5FNB	**CC**000000000 or above
MMAC-8FNB	**CG**000000000 or above
MMAC-M8FNB	**DK**000000000 or above
MMAC-M5FNB	all
MMAC-M3FNB	all

NOTE
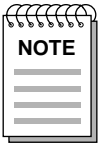
If your MMAC does not have a shunting backplane, upgrade kits are available. For additional information on shunting backplanes, or how to upgrade your hub, contact Cabletron Systems Technical Support.

1.4   ETHERNET CHANNELS A, B, C, D, E, and F

The EMM-E6 manages all Ethernet bridging traffic within its resident hub. This means that the EMM-E6 controls up to six of the Ethernet bridging channels - A, B, C, D, E, and, in the future, F. These channels access the same EMM-E6 shared memory, so bridging between channels is concurrent.

1.4.1   Ethernet Channel A

Channel A operates over the MMAC Power and Management Bus, Cabletron's original Ethernet channel. Only Cabletron Systems non-repeater MIMs (i.e., TPMIMs, FOMIMs, and THN-MIMs) access the EMM-E6 through Ethernet Channel A. Additionally, the TPXMIM Ethernet Port Assignment modules are able to communicate through Ethernet Channel A, as well as the additional backplane channels. When the EMM-E6 receives a frame on Channel A, it goes through the same bridging functions as any of the other channels. In addition, the EMM-E6 incorporates IEEE 802.3 repeater logic to repeat Channel A frames. In other words:

- the EMM-E6 bridges for all attached devices, and provides Ethernet repeating functions for Channel A modules

- even if the EMM-E6 does not bridge the Channel A traffic it receives, it still repeats the information back out onto the Ethernet A Channel.

1.4.2   Ethernet Channels B and C

The Cabletron Systems MultiChannel family of MIMs includes the Repeater Interface Controller Media Interface Module (RIC MIM), an IEEE 802.3 compliant multi-port repeater. You can configure these modules to operate on either the Ethernet Channels B or C, or as a standalone repeater, using hardware jumpers or management software.

RIC technology provides the option of connecting multiple RIC MIMs over one common bus. This single bus connection allows multiple RIC MIMs, communicating over an inter-RIC bus, to act as a single logical repeater. For example:

- An Ethernet frame follows a path from one RIC MIM, to the inter-RIC bus, to another RIC MIM.

- The RIC MIM retimes and regenerates the frame before transmitting it to all ports.

Using this configuration yields a path cost equivalent to only one repeater hop. Since the limit of serially linked repeaters in an Ethernet network is only four, using the RIC repeater offers a significant advantage. By using cascading RIC MIMs it is possible to construct a much larger network than you could with stand-alone repeaters.

Channels B and C traffic travels through RIC MIMs (i.e., TPRMIMs, FORMIMs, and CXRMIMs). These MIMs repeat packets on their own, without the EMM-E6. Ethernet Channels B and C handle network traffic over the RIC management bus on the FNB.

When frames have destination addresses for the same bus:

- the sending RIC MIM transmits the frames over its designated Ethernet bus;

- the other RIC MIMs on this bus receive the frames, and repeat them;

- the EMM-E6 receives the frames and, after determining the destination, filters the frame.

When frames have destination addresses for a different bus:

- the sending RIC MIM transmits the frames over its designated Ethernet bus;

- the other RIC MIMs on this bus receive the frames, and repeat them;

- the EMM-E6, after determining the source and destination, forwards the traffic accordingly.

In addition to providing management for these modules, the EMM-E6 also gathers Network, Board, and Port Level performance and error statistics for each individual RIC MIM on Channels B and/or C.

1.4.3   Other FNB Modules

Third Party MIMs - The EMM-E6 recognizes the third party MIMs listed below and provides each module with support concerning the statistics on the backplane and the control of channel selection for the entire module:

- **CSMIM2 -** With supported connectivity for Channels A, B, or C in an FNB chassis.
- **MODMIM -** With supported connectivity for Channels A, B, or C in an FNB chassis.
- **CRM-3E -** With supported connectivity for Channels A, B, or C in an FNB chassis.
- **PCMIM -** With supported connectivity for Channel A in any MMAC chassis.
- **SNACMIM-E** - With supported connectivity for Channel A in any MMAC chassis.

FDDI and Token Ring Modules - The EMM-E6 recognizes the following FDDI and Token Ring modules, but the EMM-E6 management does not provide control or statistics.

- **CRM-3T**
- **SNACMIM**
- **TRMIM-32A**
- **TRMIM-34A**
- **TRRMIM-F2T**
- **TRRMIM-F3T**

With TRMMIM version 2.02 or greater, both Token Ring and Ethernet modules can reside in the same chassis and support physical management capabilities of the Token Ring MIMs using the TRMMIM as the Token Ring management module. Without the TRMMIM, the EMM-E6 will only recognize the Token Ring modules.

TPXMIM - The EMM-E6 also supports Cabletron's family of Twisted Pair Switching Media Interface Modules (TPXMIMs). These modules provide board or individual port connectivity to any MMAC-FNB Ethernet channel (A, B, or C) with full SNMP management including RMON. All ports initially default to Channel B upon power up and require a Management Information Base (MIB) change to access any other channel.

1.4.4   Ethernet Channel D

Ethernet Channel D is provided by one of the two redundant EPIM ports on the front panel of the EMM-E6. These EPIM ports provide the capability for the use of a variety of Ethernet transmission media connections, including twisted pair, fiber optic, and thick or thin Ethernet coaxial cable.

Either one of the EPIM ports can act as the bridge port to the external network. When the EMM-E6 is first powered up, the EPIM 1 port acts as the bridge port and the EPIM 2 port is off. Using the network management capabilities of the EMM-E6, you can reverse this configuration to have the EPIM 2 port act as the primary bridge port.

Only one EPIM operates at any given time. However, using both EPIM slots in a redundancy configuration ensures that if the primary bridging port fails, or the connecting cable segment becomes inoperable, the backup port automatically takes over the bridging operation. This is referred to as Front Panel Redundancy.

As it does for Channels B and C, the EMM-E6 only bridges (i.e., it does not repeat) Channel D traffic. When the EMM-E6 receives a frame destined for Channel D, it goes through the normal bridging process for that frame and filters/forwards the information accordingly.

1.5 CHANNELS E AND F

The EMM-E6 provides interfaces for two optional Bridge Router Interface Modules (BRIMs). These modules provide the EMM-E6 with additional connectivity for either bridging or routing functions. At the same time, BRIMs provide access to various transmission methods.

As bridging modules, BRIMs perform the same functions as EPIMs; they transfer packets between different channels. However, unlike EPIMs, BRIMs bridge these packets from one transmission type to another (e.g., Ethernet to FDDI).

1.6 BRIDGES

An Ethernet bridge is a device that allows the expansion of a network beyond the limitations of the IEEE 802.3 specified limits for repeated Ethernet networks. If an Ethernet network has a repeater hop of four repeaters or a round trip propagation delay near the 51.2 μs maximum, a bridge can be used to build an extended network. Ethernet bridges read in packets and decide to filter or forward based on the destination address of the packet. The simple forward/filter decision process allows a bridge to segment traffic between two networks, keeping local traffic local. This process increases the availability of each network while still allowing traffic destined for the opposite side of the bridge to pass.

Bridges can also connect similar networks together such as Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) together. Note that similar networks means that the upper five layers of the OSI model, see Figure 1-2, are the same but that different Data Link and Physical layers may be used by the architecture. The Bridge operates at the Data Link level of the OSI model. It stores packets and based on the packet destination address, forwards or filters the packets. Because bridges work at layer 2 of the OSI model, bridges are protocol independent. A bridge must read the complete data frame, check for errors, and make forward or filter decisions based on recognized addresses stored in its source address table.
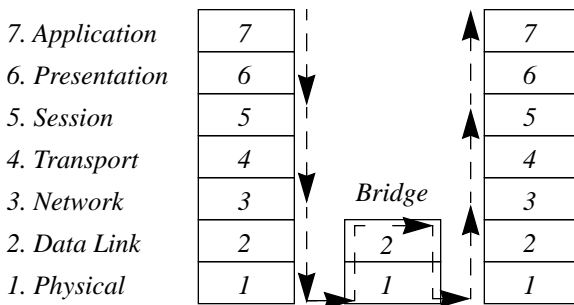
Figure 1-2. OSI Model

The bridge is considered a node on the network and performs store and forward functions for packets on each network. This contrasts with a repeater which repeats the signal bit by bit from one side of the network to the other. The bridge actually reads each packet, checks the packet for accuracy, then decides whether the packet should be sent to the other network based on the destination address. If the other network is busy, it is the responsibility of the bridge to store the packet, for a reasonable time, until the transmission can be made.

The bridge is also responsible for handling collisions. If a collision happens as the bridge is transmitting onto the second network, the bridge is responsible for the back off and retransmission process. The original sending node is not made aware of the collision. It assumes the packet has been sent correctly. If the bridge is unable to send the packet to its final destination, the original sending station, expecting some response from the device it was attempting to contact, will "time out" and, depending on the protocol attempt retransmission.

1.6.1 Filtering and Forwarding

The bridge decides whether to forward or filter a packet based on the physical location of the destination device with respect to the source device. A bridge dynamically learns the physical location of devices by logging the source addresses of each packet and the bridge port the packet was received on in a table called the Source Address Table (SAT).

1.6.2   Spanning Tree Algorithm

The Spanning Tree Algorithm (STA) is used by bridges to detect data loops (duplicate data paths). The bridges will then automatically break the loop and use the now open path as a backup in case the primary path fails.

When a bridge is powered up, it goes through a series of self tests to check its internal operation. During this time the bridge is in a standby, or **blocking**, condition and does not forward traffic. Also during this standby period, the bridge sends out special bridge management packets called configuration Bridge Protocol Data Units (BPDU). Bridges use the BPDUs as a way of communicating with each other. The purpose of the configuration BDPU is to notify other bridges on all of the connected networks of the current topology.

After the bridge has informed the network of its presence, the bridge enters a second standby state, called **listening**. During listening, the bridge monitors the network for the BPDUs of other bridges. Having received packets from the networks, the bridge enters the **learning** state, continuing to block traffic as it examines the information it receives.

Based on bridge priorities and MAC addresses, the interconnected bridges will set bridge ports to either **forwarding** or **standby** conditions, allowing a single access path to all parts of the network. The bridge or bridges involved in this primary data path will then remain in the forwarding state, and the bridges with lower priority involved in the backup path(s) will remain in a standby condition. Any redundant paths (those placed in standby) will be automatically used as need is detected by the operation of the Spanning Tree Algorithm.

The other type of BPDU is the topology change BPDU. This BPDU is made up of four bytes and notifies the other bridges that a change has taken place. Upon receipt of the topology change BPDU, the bridges re-arbitrate, or re-span, to form a legal topology.

1.7   LOCAL MANAGEMENT FEATURES

Local Management for the EMM-E6 provides tools that allow you to manage the device and its attached segments. Through Local Management you can:

- Assign an IP address and subnet mask to the EMM-E6 bridge via the Configuration Screen menu.

- Select a default gateway and default interface.

- Control EMM-E6 local and remote access by establishing Community Names.

- Designate which Network Management Workstations receive SNMP traps from the EMM-E6.

- Navigate through Management Information Bases (MIBs). Since the EMM-E6 is an SNMP compliant device, you can manage related SNMP MIB objects, given the appropriate security level. You can also manage the IETF Bridge MIB objects and many of the RMON (Remote Monitoring) MIB objects.

Other management capabilities include enabling and unlocking all managed ports in the Multi Media Access Center (MMAC) chassis.

1.8   COMMUNITY NAMES

When using Local or Remote Management tools to access the EMM-E6 it is important that the Network Manager has the ability to maintain network security. Community Names provide some network security by acting as passwords into the device and the software running it. The Network Manager (Super-user) controls access by establishing four (4) passwords. Each of these passwords is associated with a specific level of access to the Local Management capabilities of the EMM-E6. The Community Names are set through the Local Management Community Name Table. Once these are set by the Network Manager, they can be maintained in confidence or limited to users who have a need to manage the system. The four levels of access are:

- Super-User - Allows full management privileges
- Read-Write - Allows editing of device configuration parameters not including changing Community Names
- Read-Only - Allows reading of device parameters not including Community names
- Basic-Read - Allows reading low level device data

1.9   SNMP

SNMP (Simple Network Management Protocol) is a protocol within the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. Network applications such as Local Management and MIB Navigator use SNMP to manage device configurations and monitor operating conditions. SNMP protocol defines methods for "GETs," "SETs," and "TRAPs," either remotely from any point along the TCP/IP network or locally. This allows for control of the device from any point along the network. SNMP tools use the MIBs located on the device to be managed to; access information (GET), change device parameters (SET), and to notify previously selected users that an event has occurred (TRAP).

1.9.1   MIBs

The Management Information Bases (MIBs) are a database resident on the EMM-E6. Objects in the information base are uniquely identified by administratively assigned identifiers (called object identifiers or OIDs), and can be viewed, retrieved, or changed using an SNMP packet exchange over the network.

1.10   REVIEW OF ADDRESSING

For network devices to recognize one another, unique identifiers, referred to as addresses, are required. The following sections are intended for review, and do not represent a comprehensive description of network addressing.

This section begins by discussing the two types of addressing used in TCP/IP networks, Internet Protocol (IP) addresses and Media Access Control (MAC) addresses. These descriptions are followed by an overview of the process of configuring addresses in a network, including examples of network Classes and the creation of subnets within networks.

1.10.1   MAC Addresses

The MAC address is a unique, 48-bit binary number, associated with a specific physical connection to a network which is capable of generating packets. Examples of devices with MAC addresses include SNMP agents and DNI cards. MAC addresses are divided into 6 octets, and represented in hexadecimal form such as the following:

00-00-1D-00-26-FB

All MAC addresses are administered by the IEEE and are generally assigned at the time of manufacture, and cannot be changed. The first three octets uniquely identify the manufacturer. Cabletron devices' MAC addresses all start with: **00-00-1D.**

As MAC addresses are often used to perform management and control functions for networking hardware, it is important to be able to identify a MAC address when it is requested or returned by network management. Since most MAC addresses are set at manufacture and cannot be altered by users, this manual does not examine MAC addressing in greater detail.

1.10.2   IP Addresses

Each network interface or TCP/IP host is identified by a 32-bit binary number called the Internetwork Protocol (IP) address. An IP address represents a connection to the network, but does not identify any specific physical device location (physical locations are determined by MAC Addresses, discussed earlier in this chapter). Every IP address is made up of four 8-bit binary numbers (octets). Each octet is translated into its decimal equivalent and represented using Dotted Decimal Notation (DDN). The DDN format is **XXX.XXX.XXX.XXX**. Any of the four DDN values, called fields, can range from **1** (octet 0000 0001) to **255** (octet 1111 1111). An IP address is made up of two portions, the Network ID and a Host ID. Network IDs refer to a particular network and are assigned by the Internet Assigned Numbers Authority (IANA). The IANA assigns fixed numbers to one, two, or three of the fields in order to provide a unique Network ID.

Once a Network ID has been assigned, the Network Manager assigns individual Host IDs by configuring different values (within the allowable ranges) for the octets not set by the IANA. This allows individual hosts on the network to be identified by distinct numerical addresses.

There are three classes of IP addresses which define the Network and Host ID numbering scheme. Tables 1-1 through 1-3 describe the classes. The **bold** type in these tables indicates a field assigned by the IANA, the Network ID. Any time the term "host" is found in the DDN format example address, it indicates a Host ID field, which may be assigned by the network manager.

Table 1-2. Class A

Range of Network IDs:	**1 - 126**. host. host. host [1 octet for the Network ID (127 reserved)]
Binary translation: (of first octet)	**0000001 - 0**1111111 [first bit is always 0]
Range for the Host ID:	**net**. 1 - 254. 1 - 254. 1 - 254 [3 octets for the Host ID - allows 16,777,214 hosts per network]

Table 1-3. Class B

Range of Network IDs:	**128 - 191**. **1 - 254**. host. host [2 octets for the Network ID]
Binary translation: (of first octet)	**1000000 - 10**111111 [first bit is always 1 and second is always 0]
Range for the Host ID:	**net**. **net**.1 - 254. 1 - 254 [2 octets for the Host ID - allows 65,534 hosts per network]

Table 1-4. Class C

Range of Network IDs:	**192 - 223**. **1 - 254**. **1 - 254**. host [3 octets for the Network ID]
Binary translation: (of first octet)	**1100000 - 110**11111 [first and second bits always 1 and third is always 0]
Range for the Host ID:	**net**. **net**. **net**. 1 - 254 [1 octet for the Host ID - allows 254 hosts per network]

1.10.3   Identifying IP Address Classes

In the event that you have an existing IP address and need to quickly determine what fields are available for Host IP address configuration, make that determination based on the binary value of the first DDN field. Tables 1-1 to 1-3 show that different address classes have different initial bits in the first octet. A Class A address, for example, will always have a zero as the first bit of the first octet. To identify an IP address' class, convert the decimal value of the first DDN field to binary.

Example: 132.177.118.24

Convert first DDN field to binary: $132_{10} = \underline{10}000100_2$

Since the first two bits of the octet are 10_2, the address is Class B. Refer to the IP address Classes tables, each Class B address utilizes the first two fields for a Network ID (**132**.**177**.118.24), while the remaining two fields (132.177.**118**.**24**) are the Host ID.

1.10.4   Subnet Addresses

Subnet addresses are used to partition an IP network into multiple subnetworks or subnets. The use of subnet addresses adds an additional layer of hierarchy to the IP addressing scheme. This additional addressing layer facilitates isolation, control, and administration of users within the network, at a cost of reduction in total available Host IDs. This is done by grouping hosts into separate subnets. To use the above Class B address, 132.177.118.24, as an example, the last two fields are available for the assignment of Host IDs. If the Network Manager desired to use subnets, the third field, 118, could become common to a series or group of hosts with a common physical location or intended purpose.

Example (Class B):

Net ID   Host ID

132.177.118.24

Subnet Number   *Host Number*
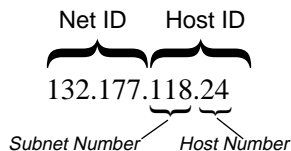
Subnet addresses, when used with routing, allow discrimination between devices and groups of devices based on IP addresses. Networks of different subnets, even those on the same physical network segment, may be isolated, from a functional standpoint, from one another through the implementation of routing. Repeaters, bridges, and switches, which operate at the Data Link layer of the OSI model, make their decisions based on MAC addresses. Network devices such as routers, servers, and client stations can use IP addressing to recognize transmissions intended for them. If a station on one routed subnet sees a transmission from another subnet, it will ignore the packet without concern over who it is intended for. To overcome this subnetwork blindness a router is used. Any station or device which implements subnet masking needs to be configured with an address for that subnet's Default Gateway. When the station or device transmits packets intended for a different subnetwork than the one it identifies itself as belonging to, the transmission is also sent to the Default Gateway, where the gateway or router will make the determination of where the packet is sent.

The use of subnet addresses on the network means using a Subnet Mask in conjunction with each IP address.

1.10.5   Subnet Masks

The purpose of the Subnet Mask is to indicate the part of the Host ID that is being used as a subnet address. By default no part of the Host ID is used, and therefore, the default or "Natural Mask" masks just the octets that comprise the Network ID. Table 1-5 shows the default masks for the four classes of IP networks.

Table 1-5. Class and Default Masks

Network Class	Length of Network ID	Default Mask
Class A	**X**.	**255**. 0. 0. 0
Class B	**X. X**.	**255**. **255**. 0. 0
Class C	**X. X. X**.	**255**. **255**. **255**. 0

The binary 1's in the mask "mask-out" the Network ID and the 0's show where the Host ID is located. When using part of the Host ID as a subnet address, define a Subnet Mask that will mask-out the bits of the Host ID that are being used as a subnet address. The calculations for the mask must be done at the bit level since in some cases, and in all cases for Class C addresses, the last octet must be split into part Host ID and part Subnet ID. Figure 1-3 below, shows the means by which a Subnet Mask blocks bits from an IP address to determine which bits are representing a Subnet ID and which represent a Host ID.

Network Actual (195. 191. 21. XXX) - Class C Network ID, assigned by IANA. This class of network allows for the creation of up to 254 Host IDs on one network.

| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | | X | X | X | X | X | X | X | X |

Default Subnet Mask (255. 255. 255. 0) - Masks out Network ID octets, allows all of final octet to be used for Host IDs.

| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Modified Subnet Mask (255. 255. 255. 224) - Masks first three bits of fourth octet, allowing a portion of the Host ID to be used for Subnet identification. This particular custom Subnet Mask allows the creation of six subnets, each having no more than thirty hosts (see Table 1-6, below) for a maximum of 180 Host IDs.

| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

Subnet Logical - Shows how final five bits of original remain for Host IDs.

| N | N | N | N | N | N | N | N | | N | N | N | N | N | N | N | N | | N | N | N | N | N | N | N | N | | S | S | S | H | H | H | H | H |

Subnet Actual (195. 191. 21. 87) - Host number 23 on Subnet number 64.

Subnet 64   Host 23

| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

Figure 1-3. Subnet Masking

If you decide to modify the default Subnet Mask in order to accommodate subnets within your network, you must determine the number of subnets you desire and how many Host IDs will be available within each configured Subnet.

The example in Figure 1-3 masks out the three high order bits of the only octet available for modification, the last octet. This provides for up to six subnets and up to 30 Host IDs within each subnet. Modifying the default mask for a Class B address (255.255.0.0) to mask out the third octet for subnet purposes (255.255.255.0) would provide up to 254 subnets each containing up to 254 Host IDs. Tables 1-7 and 1-6 show how using the mask determines the subnet and host addresses that are available from an individual octet. These tables examine the Host IDs and Subnet Addresses available from the use of custom masks in both Class B and Class C IP addresses. Bear in mind that Subnet Masks can only be modified for those fields which are not assigned to a site by the IANA.

Table 1-6. Examples of Class C Subnet Masks

Decimal Mask	Binary Equivalent	Available Subnet Addresses	Available Host IDs
192	11000000	64 and 192	1 - 62
224	11100000	32, 64, 96, 128, 192, 224	1 - 30
240	11110000	16 - 240 increments of 16	1 -14
240	11110000	16 - 240 increments of 16	1 -14
248	11111000	8 - 248 increments of 8	1 - 6
252	11111100	4 - 252 increments of 4	1 and 2
254	11111110	2 - 254 increments of 2	None
255	11111111	1 - 254	None

Table 1-7. Examples of Class B Subnet Masks

Decimal Mask	Binary Equivalent	Available Subnet Addresses	Host IDs Per Subnet
192. 0	11000000 00000000	64 and 192	16,382
224. 0	11100000 00000000	32, 64, 96, 128, 192, 224	8,190
240. 0	11110000 00000000	16 - 240 increments of 16	4,094
248. 0	11111000 00000000	8 - 248 increments of 8	2,046
252. 0	11111100 00000000	4 - 252 increments of 4	1,022
254. 0	11111110 00000000	2 - 254 increments of 2	510
255. 0	11111111 00000000	1 - 254	254
255. 128	11111111 10000000	0 - 255.128 1 - 255. 0	126
255. 192	11111111 11000000	0 - 254. 192 0 - 255. 128 0 - 255. 64 1 - 255. 0	62
255. 224	11111111 11100000	0 - 255. 32, 64, 96, 128, 160, 192, 224 0 - 254. 224 1 - 254. 0	30
255. 240	11111111 11110000	0 - 254. 240 0 - 255. 16 - 240 increments of 16 1 - 255. 0	14
255. 248	11111111 11111000	0 - 255. 8 - 240 increments of 8 0 - 254. 248	6
255. 252	11111111 11111100	0 - 255. 4 - 248 increments of 4 0 - 254. 252	2

1.10.6   Operation of the Subnet Mask

The Subnet Mask defines how your EMM-E6 treats SNMP Trap IP destination addresses in its Trap table (see Chapter 7, **Trap Table Screen**, for additional information on traps).

When using the Subnet Mask, the EMM-E6 logically determines one of two possible locations, either **on** or **not on** its own subnet, for each Trap IP destination address in its trap table. If the address is **on** its own subnet, the EMM-E6 transmits directly to the workstation with that address. If the address is **not on** its subnet, the EMM-E6 transmits to the workstation with that address combined with the Default Gateway IP address. Default Gateways are discussed later in this chapter.

Modify the default Subnet Mask for the EMM-E6 when workstations in the Trap table reside on a different subnet (i.e., across a gateway or external router), and you want these workstations to receive SNMP Traps generated by the EMM-E6. Caution should be exercised when configuring subnets, as a poorly subnetted network can greatly increase network traffic by duplicating transmissions.

1.10.7   Default Gateway

The Default Gateway is the IP address of the network or host to which all packets addressed to unknown networks or hosts are sent. The Default Gateway should be a perimeter or border device that connects the network with the rest of the world. The Default Gateway attempts to route the packet to the correct destination. This gateway is often used by managers to handle all traffic between private networks and the Internet. If a Default Gateway is not defined, the packets addressed to a network or host address not found in the forwarding table will be dropped.

1.10.8 Addressing Example

A network manager, planning for the configuration of a network of 60 hosts, desires to implement subnets to create logical divisions between different groups of workstations and devices. The Internet Assigned Numbers Authority has supplied the company with a Class C Network Address; 222. 131. 99. XXX.

Examining Table 1-6 for subnet masking forms, the Network Manager decides that, due to the extent of subnetting to be implemented, the last option in the subnet table is not realistic, as that configuration offers only two subnets. Likewise, the first three options are unacceptable, as they would create an excessively large number of subnets with relatively few individual hosts per subnetwork. This leaves decimal masks of 248 (31 subnets, 6 hosts each), 240 (15 subnets, 14 hosts each), and 224 (6 subnets, 30 hosts each). Any of these decimal masks would support the number of Host IDs to be configured. Looking ahead, the Network Manager realizes that adding Host IDs to a full network can involve a total reconfiguration of subnet strategies, and opts for the decimal mask 240, which provides room for the configuration of 210 Host IDs.

NOTE
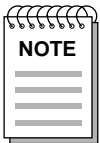
On any subnet, one Host ID must be reserved for a connection to the router(s) which will interconnect multiple subnets.

After taking time to fully plan and delineate the required subnets, assign them to departments within the company, plan out the initial Host IDs for existing devices within those subnets and configure the router(s) which will interconnect the various subnets, the Network Manager determines where on the network the network management station will reside. The IP Host ID of this network management station will be essential when configuring the network devices for sending SNMP Traps.

For any SNMP Trap-generating network devices not residing on the same subnet as the network management station, the default Subnet Mask utilized on that device must be altered to match the subnet scheme. In the above example, the default Subnet Mask is modified from 255. 255. 255. 0 to 255. 255. 255. 240. For each SNMP Trap-generating device with a modified Subnet Mask, a Default Gateway is assigned. In the event that any of the custom-masked devices generated an SNMP Trap for the network management station, a comparison of the Subnet Mask and the Network ID indicates that the SNMP Trap should be sent to that subnet's Default Gateway to be routed to the subnet where the network management station resides. The procedures for modifying the Subnet Mask and configuring the Default Gateway through Local Management may be found in Chapter 7 of this User's Guide, which deals with the Configuration Screen.

1.11   LANVIEW LEDs AND RESET SWITCH

The EMM-E6 incorporates the Cabletron Systems LANVIEW Status Monitoring and Diagnostics System. LANVIEW LEDs can help diagnose any problems, such as a power failure or a cable fault. The module includes the following LANVIEW LEDs:

- A CPU (Central Processing Unit) LED, for board status
- STBY (Standby), RCV (Receive), XMT (Transmit), and CLN (Collision) LEDs for Ethernet Status
- Power LEDs for the two EPIM slots.

The front panel also has a reset switch which allows you to re-initialize the processor. Chapter 14, **Troubleshooting**, provides detailed descriptions of each EMM-E6 LANVIEW LED.

1.12   LANVIEWSECURE

The EMM-E6 supports the LANVIEWSECURE suite of Ethernet MMAC modules. The LANVIEWSECURE products support both inbound data (Intruder Prevention) and outbound data (Eavesdrop Prevention). These products are identified by the words "LANVIEWSECURE" printed on the faceplate of the product.

Intruder prevention allows ports on the modules to be configured with expected MAC addresses. If a port receives a packet from a station or device whose MAC address does not correspond to the one previously associated with that port, the port will automatically lock, sensing the presence of an unauthorized station, then generate and send a trap to the Network Management station to indicate the intruder violation.

Eavesdrop prevention delivers a modified data portion (filled with a random pattern of binary ones and zeroes) to all ports on the module except the port specified in the original packet's destination MAC address field. Effectively, all ports, except the destination port, recognize the presence of a packet, but receive meaningless information.

LANVIEWSECURE modules also provide a "Full security" configuration, under which broadcast and multicast packets contain modified data fields such as those used in eavesdrop prevention (described above). Ports set to Full security mode will not see or respond to these types of packets. The default setting for Full security is disabled. Enabling the Full security function modifies the broadcast and multicast packets.

LANVIEWSECURE is enabled upon the locking of a channel, module, or port. When enabled, the first two addresses that are learned become the expected addresses associated with that port on any LANVIEWSECURE module. If a port has never been enabled and a MAC address is added to that port, then any MAC address learned on that port will be deleted automatically. If a port is enabled and a new address is added to that port, then any existing addresses remains in the expected address table.

1.13   GETTING HELP

If you need additional support related to installation, configuration, or management of the EMM-E6, or if you have any questions, comments, or suggestions concerning this manual, contact Cabletron Systems Technical Support:

By phone.......................... (603) 332-9400
                                              Monday-Friday; 8am - 8pm ET

By CompuServe............... GO CTRON from any ! prompt

By Internet mail............... support@ctron.com

1.14   RELATED MANUALS

Use the following manuals to supplement the procedures and other technical data provided in this manual. This manual references procedures in these manuals, where appropriate, but does not repeat them.

Cabletron Systems' **MMAC Overview and Setup Guide**

Cabletron Systems' **Bridge Router Interface Module Guide(s)**

Cabletron Systems' **Repeater Interface Controller Media Interface Modules (TPRMIM/FORMIM/CXRMIM) Installation Guide**

Cabletron Systems' **Remote LANVIEW/Windows Network Control Management for the Cabletron Systems Station Software User's Manual**

Cabletron Systems' **Router Services Manuals**

CHAPTER 2

REQUIREMENTS / CONFIGURATIONS

This chapter contains general networking guidelines. Before attempting to install the EMM-E6 or any additional EPIMs or BRIMs, review the requirements and specifications outlined in this chapter.

> ⚠️ **CAUTION**
>
> *Your network installation must meet the conditions, guidelines, specifications, and requirements included in this chapter to ensure satisfactory performance of this equipment. Failure to follow these guidelines may produce poor network performance.*

2.1 NETWORK REQUIREMENTS

Take care in planning and preparing the cabling and connections for your network. The quality of the connections, the length of cables, and other conditions of the installation play critical roles in determining the reliability of your network.

Refer to sections below that apply to your specific network configuration.

2.1.1   10BASE-T Twisted Pair Network

When connecting a 10BASE-T segment at any of the 10BASE-T hub ports or a 10BASE-T Ethernet Port Interface Module (EPIM-T), ensure that the network meets the following requirements:

*   **Length** - The IEEE 802.3 10BASE-T standard requires that 10BASE-T devices transmit over a 100 meter (328 foot) link using 22-24 AWG unshielded twisted pair wire. However, cable quality largely determines maximum link length. If you use high quality, low attenuation cable, it may be possible achieve link lengths of up to 200 meters. Cable delay limits maximum link length to 200 meters, regardless of the cable type.
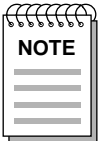
> **NOTE**
>
> *Losses introduced by connections at punch-down blocks and other equipment reduce total segment length. For each connector or patch panel in the link, subtract 12 meters from the total length of your cable.*

*   **Insertion Loss** - Between frequencies of 5.0 and 10.0 MHz, the maximum insertion loss must not exceed 11.5 dB. This includes the attenuation of the cables, connectors, patch panels, and reflection losses due to impedance mismatches in the link segment.

*   **Impedance** - Cabletron Systems 10BASE-T Twisted Pair products work on twisted pair cable with 75Ω to 165Ω impedance. Unshielded twisted pair cables typically have an impedance of between 85Ω and 110Ω. You can also use shielded twisted pair cables, such as IBM Type 1 cable, but keep in mind that this cable has an impedance of 150Ω.

    The high impedance of the IBM Type 1 cable increases signal reflection. However, due to cable shielding, and its subsequent lack of crosstalk between shielded pairs, this signal reflection has little effect on the quality of the received signal.

• **Jitter** - Intersymbol interference and reflections can cause jitter in the bit cell timing, resulting in data errors. 10BASE-T links must not generate more than 5.0 ns of jitter. Make sure your cable meets 10BASE-T link impedance requirements to rule out jitter as a concern.

• **Delay** - The maximum propagation delay of a 10BASE-T link segment must not exceed 1000 ns. This 1000 ns maximum delay limits the maximum link segment length to no greater than 200 meters.

• **Crosstalk** - Signal coupling between different cable pairs within a multi-pair cable bundle causes crosstalk. 10BASE-T transceiver design alleviates concerns about crosstalk, providing the cable meets all other requirements.

• **Noise** - Crosstalk, or externally induced impulses, are causes of noise. Impulse noise may cause data errors if the impulses occur at very specific times during data transmission. Generally, noise is not a concern. If you suspect noise-related data errors, you may need to reroute the cable or eliminate the source of the impulse noise.

• **Temperature** - Multi-pair PVC 24 AWG telephone cables typically have an attenuation of approximately 8-10 dB/100 m at 20°C (78°F). The attenuation of PVC insulated cable varies significantly with temperature. At temperatures greater than 40°C (104°F), we strongly recommend using plenum-rated cable to ensure attenuation remains within specification.

2.1.2   Multimode Fiber Optic Network

When connecting a multimode fiber optic link segment to the hub (via EPIM-F1/F2), ensure the network meets the following requirements:

- **Cable Type** - Use the EPIM-F1 and EPIM-F2 for the following multimode fiber optic media:

    - 50/125 µm fiber optic cabling
    - 62.5/125 µm fiber optic cabling
    - 100/140 µm fiber optic cabling

- **Attenuation** - You must test the fiber optic cable with a fiber optic attenuation test set adjusted for an 850 nm wavelength. This test verifies that the signal loss in a cable falls within the following acceptable levels:

    - 13.0 dB or less for a 50/125 µm fiber cable segment
    - 16.0 dB or less for a 62.5/125 µm fiber cable segment
    - 19.0 dB or less for a 100/140 µm fiber cable segment

- **Budget and Propagation Delay** - When you determine the maximum fiber optic cable length to incorporate fiber runs into your network, you must calculate and consider the fiber optic budget (a total loss of 10.0 dB or less is permissible between stations) and total network propagation delay.

    To determine the fiber optic budget, combine the optical loss due to the fiber optic cable, in-line splices, and fiber optic connectors. Typical loss for a splice and connector (together) equals 1 dB or less.

    Total propagation delay allowed for the entire network must not exceed 25.6 µs in one direction (51.2 µs round trip). If the total propagation delay between any two nodes on the network exceeds 25.6 µs, you must either reduce the delay or use a bridge.

- **Length** - The maximum possible multimode fiber optic cable length is 2 km (2187.2 yards). However, IEEE 802.3 FOIRL specifications specify a maximum of 1 km (1093.6 yards).

2.1.3   Single Mode Fiber Optic Network

When connecting a single mode fiber optic link segment to the hub (via EPIM-F3), ensure the network meets the following requirements:

- **Cable Type** - Fiber optic link segments should consist of 8/125 to 12/125 μm single mode fiber optic cabling. You can also use 62.5/125 μm multimode cable with the EPIM-F3; however, multimode cable has greater optical loss, and limits the possible distance to 2 km.

- **Attenuation** - You must test the fiber optic cable with a fiber optic attenuation test set adjusted for a 1300 nm wavelength. This test verifies that the signal loss in a cable falls within the acceptable level of 10.0 dB or less for any given single mode fiber optic link.

- **Budget and Propagation Delay** - When you determine the maximum fiber optic cable length to incorporate fiber runs into your network, you must calculate and consider the fiber optic budget (a total loss of 10.0 dB or less is permissible between stations) and total network propagation delay.

  To determine the fiber optic budget, combine the optical loss due to the fiber optic cable, in-line splices, and fiber optic connectors. Typical loss for a splice and connector (together) equals 1 dB or less.

  Network propagation delay is the amount of time it takes a packet to travel from the sending device to the receiving device. Total propagation delay for the entire network must not exceed 25.6 μs in one direction (51.2 μs round trip). If the total propagation delay exceeds 25.6 μs, you must use bridges.

- **Length** - If you meet all system budgets, the maximum single mode fiber optic cable length can reach 5 km (3.1 miles) with bridges at each segment end. However, IEEE 802.3 FOIRL specifications specify a maximum of 1 km (1093.6 yards).

2.1.4   Thin-net Network

When connecting a thin-net (coaxial) segment to your hub (via an
EPIM-C), ensure your network meets the following requirements:

- **Cable Type** - Use only 50 ohm RG-58A/U type coaxial cable for
  thin-net cable segments.

- **Length** - The thin-net segment must not exceed 185 meters.

- **Terminators** - Terminate each end of a thin-net segment.

- **Connectors** - You can use up to 29 T-connectors throughout the
  length of the cable segment for host connections.

  If you use an excessive number of barrel connectors within the cable
  segment (e.g., finished wall plates with BNC feed-throughs), you
  may need to reduce the number of host connections. For special
  network design, contact Cabletron Systems Technical Support.

- **Grounding** - For safety, ground only **one** end of a thin-net segment.
  Do NOT connect EPIM BNC ports to earth ground.
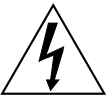
> *Connecting a thin-net segment to earth ground at more than one
> point could produce dangerous ground currents.*

2.2   TRANSCEIVER REQUIREMENTS

When you connect an external network segment to an EPIM-A in your
hub through a transceiver, that transceiver must meet IEEE 802.3
standards or Ethernet version 1.0 or 2.0 requirements. The transceiver
must also have SQE disabled.

2.3   REPEATER MEDIA INTERFACE MODULES

The EMM-E6 communicates with the Repeater MIMs over Ethernet Channels B and C of the MMAC-FNB. The following repeater MIMs are currently available:

- **CXRMIM**: coaxial repeater MIM; twelve 10BASE-2 coaxial connectors; one EPIM.

- **FORMIM-22**: fiber optic repeater MIM; twelve FOIRL/ 10BASE-FL ports; ST type connectors.

- **TPRMIM-20/TPRMIM-22**: twisted pair repeater MIM; RJ45 connectors (TPRMIM-20 has nine, TPRMIM-22 has twenty-one); one EPIM.

- **TPRMIM-33/TPRMIM-36**: twisted pair repeater MIM; 50-pin RJ71 connectors (TPRMIM-33 has one, TPRMIM-36 has two); each RJ71 connector provides twelve 10BASE-T twisted pair ports (twelve total for TPRMIM-33, twenty-four total for TPRMIM-36); each MIM has one EPIM; the TPRMIM-36 also has one AUI port.

For more information regarding Cabletron Systems Repeater MIMs, refer to your **Repeater Media Interface Modules (TPRMIM/FORMIM/ CXRMIM) Installation Guide**.

2.4   PORT ASSIGNMENT MODULES

- **TPXMIM-20/TPXMIM-22**: twisted pair port and bank assignment repeater MIM; RJ45 connectors (TPXMIM-20 has nine, TPXMIM-22 has twenty-one); one EPIM.

- **TPXMIM-32/TPXMIM-36**: twisted pair port and bank assignment repeater MIM; RJ71 connectors (TPXMIM-32 has one, TPXMIM-36 has two); one EPIM.
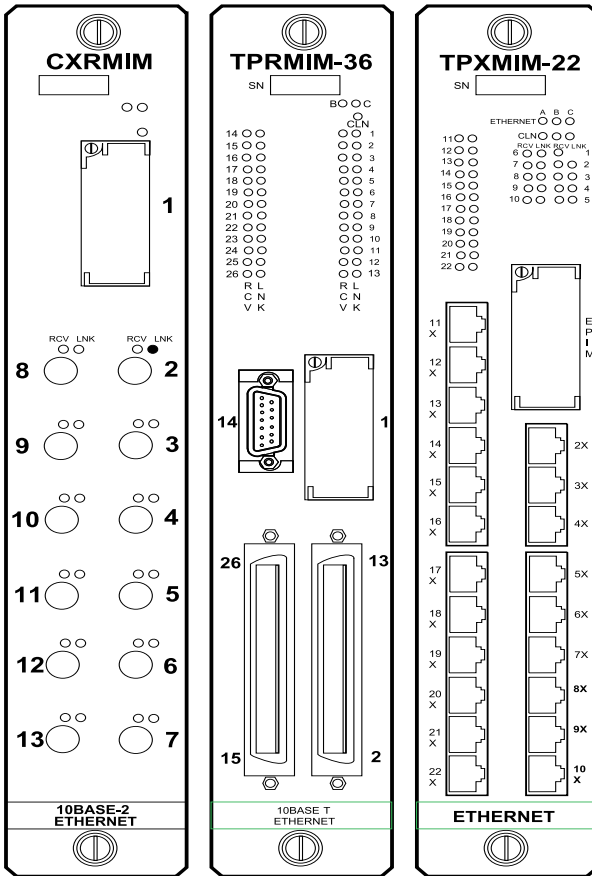
Figure 2-1. Sample Repeater MIMs

2.5   SAMPLE NETWORK CONFIGURATIONS

This section provides you with several examples for configuring networks with the EMM-E6. These examples illustrate the flexibility and advantages to using the EMM-E6 and RIC MIM technology:

2.5.1   Three networks with a single MMAC-FNB
2.5.2   The EMM-E6 as a multi-port router
2.5.3   Adding users to an existing network
2.5.4   A fault tolerant wiring scheme
2.5.5   The EMM-E6 and BRIMs

2.5.1   Three Networks With a Single MMAC-FNB

One of the basic applications of the EMM-E6 is for configuring three separate networks within one MMAC. This provides you with the advantages of having three separate networks in one wiring closet, with full bridging and SNMP management for each network. Figure 2-2 illustrates an example of the three network configuration.
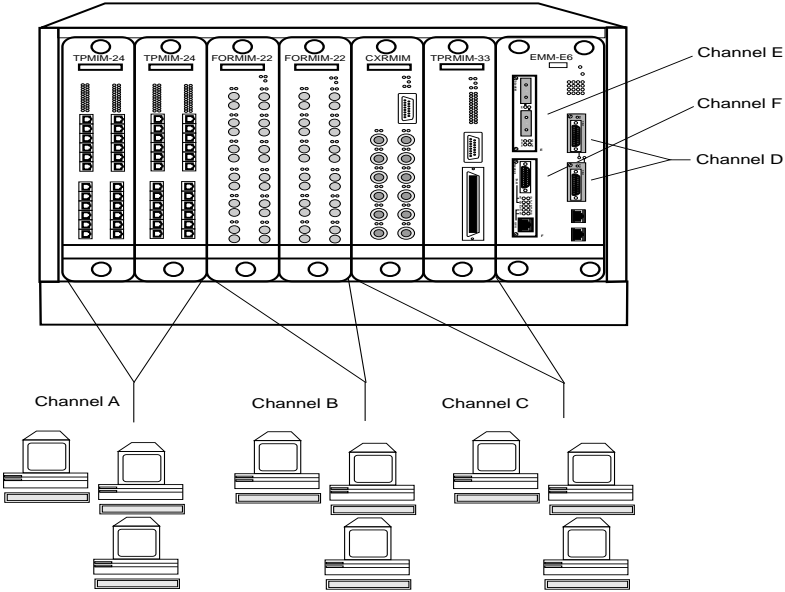
Figure 2-2. Single MMAC-FNB Configuration

2.5.2   The EMM-E6 as a Multiport Router

An EMM-E6 routing image allows you to set up the module as a multi-port router. For information on how to upgrade the EMM-E6 to perform routing functions, and how to configure the EMM-E6 as a multi-port router, refer to Cabletron Systems' **Router Services Manual** or contact Cabletron Systems Technical Support.

2.5.3 Adding Users to a Separate Segment

The example in Figure 2-3 compares two methods of connecting 48 additional users to a network.
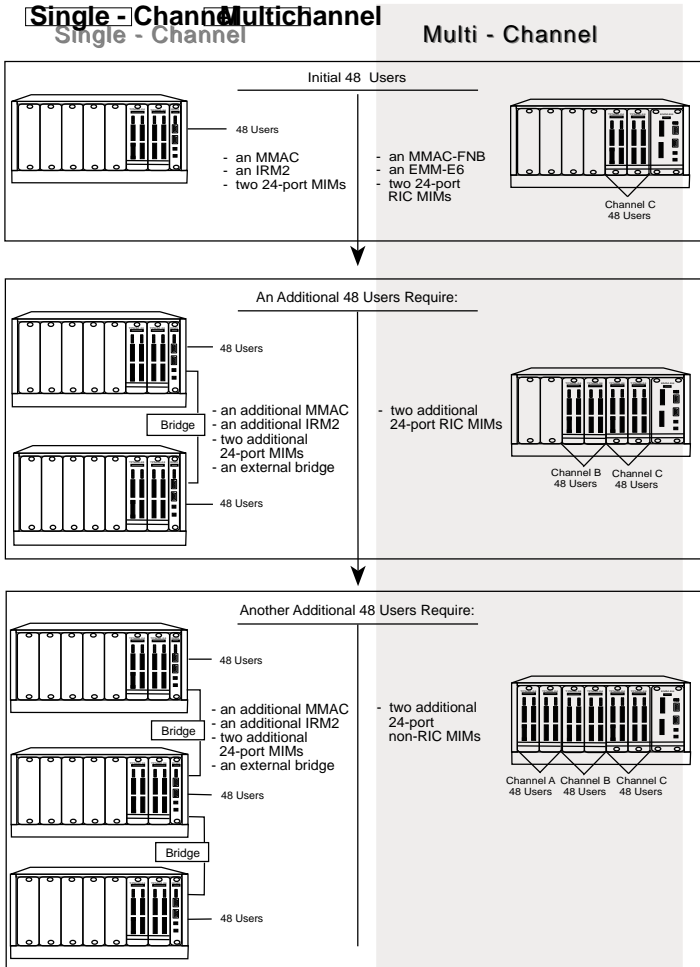
Figure 2-3. Adding New Users

To place additional users on a new network with an EMM-E6, you only need to add a few additional MIMs to the MMAC-FNB.

2.5.4   A Fault Tolerant Wiring Hierarchy

The example in Figure 2-4 illustrates a fault tolerant wiring hierarchy.
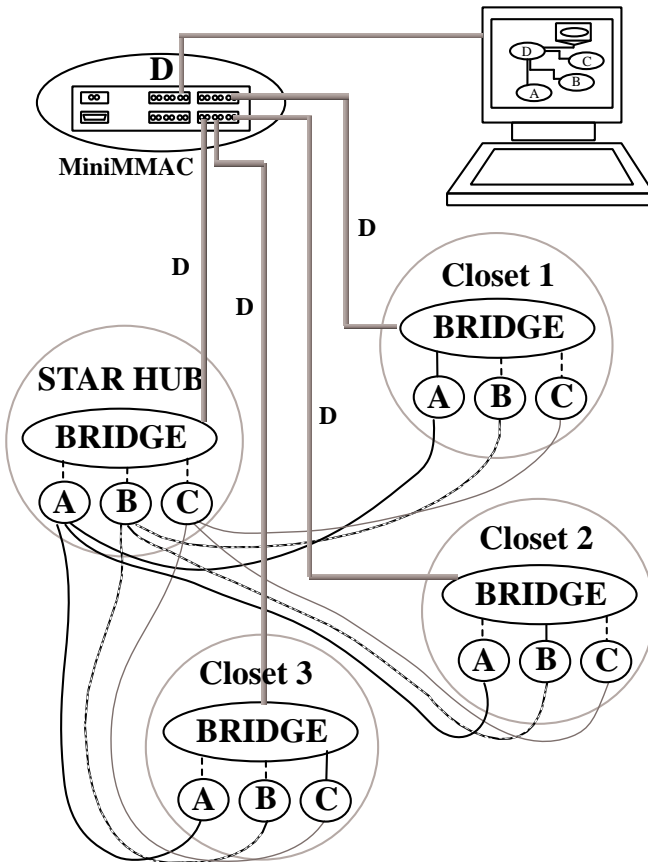
Figure 2-4. Configuring a Fault Tolerant Wiring Scheme

Closets 1, 2, and 3 each contain an MMAC-FNB with an EMM-E6, MIMs, and RIC MIMs operating on Ethernet channels A, B, and C. Within each closet, each Ethernet channel is separately repeated, and each is dedicated to a specific set of network users (for example, Ethernet A contains Novell users, Ethernet B contains TCP/IP and NFS users, and Ethernet C contains DECnet users).

The Star Hub, which is an MMAC-FNB that uses a configuration similar to the closet hubs, is the central repeater interconnect for the closets, but does not constitute a single point of failure.

The EMM-E6 in each MMAC-FNB utilizes the 802.1d Spanning Tree Algorithm. By configuring the Root Path Cost and the Bridge Priority on the EMM-E6, you can bridge primary paths from each segment to Network D from each EMM-E6 (indicated by the solid line between Ethernet channel A and the bridge in closet 1, Ethernet channel B and the bridge in closet 2, and Ethernet channel C and the bridge in closet 3). The dotted lines between the other Ethernet channels and the bridge show the backup paths in a standby condition. If any repeater link fails, or if an active bridge path fails, one or many backup bridge paths may become active, replacing the failed repeater link or bridge path.

An additional level of redundancy is achieved by using the cable redundancy algorithm built into Cabletron's EMM-E6. This feature enables you to configure redundant bridge paths, with one path remaining in backup, standby mode until the primary path fails.

In the example, Segment D provides a manageable backbone, using a MiniMMAC. Segment D provides intercommunication for channels A, B, and C, as well as serving as the network management segment for the hierarchy. The individual protocol segments are filtered by the EMM-E6 bridge component, so that the only traffic on segment D is minimal inter-channel communication (i.e., mail). Otherwise, only network management data is on segment D, out-of-band of the traffic on channels A, B, and C.

2.5.5   The EMM-E6 and BRIMs

The example in Figure 2-5 illustrates just one possible EMM-E6 and
BRIM configuration. The EMM-E6/BRIM combination provides various
connection possibilities, depending on the BRIM(s) you use. Refer to
individual BRIM manuals and/or Cabletron Systems' **Router Services**
documentation to better understand the capabilities of each device.
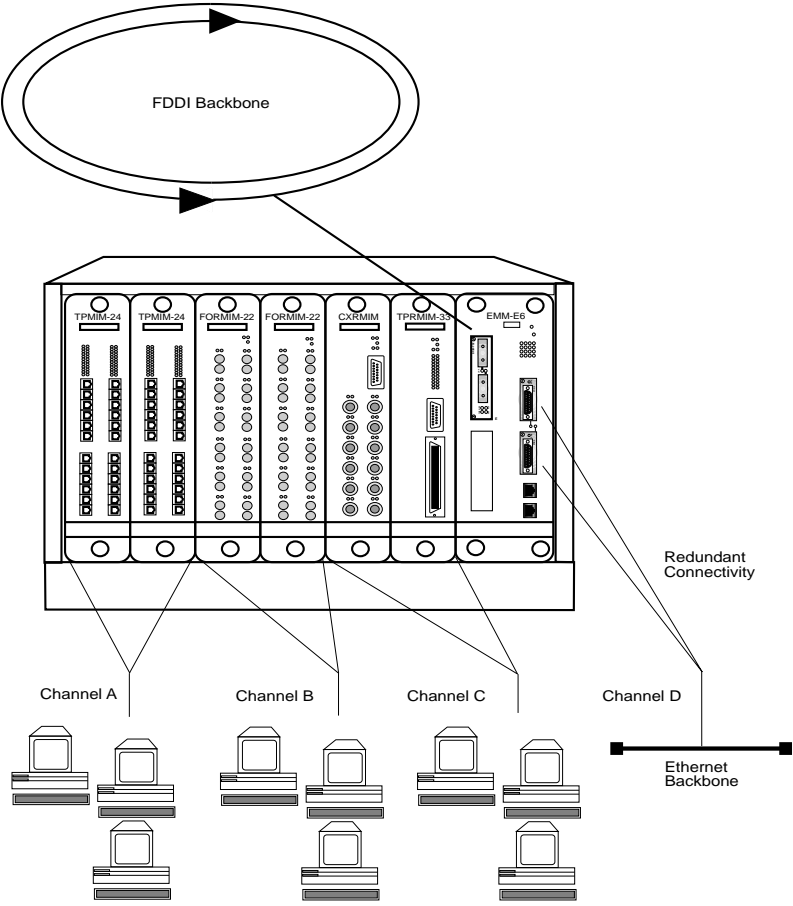
Figure 2-5. The EMM-E6 and BRIMs

CHAPTER 3

INSTALLATION

This chapter contains instructions for:

- unpacking and inventorying the contents of the EMM-E6 carton

- locating, identifying and setting the EMM-E6 mode switches

- adding/replacing optional modules (i.e., Single In-line Memory Modules and Ethernet Port Interface Modules)

- identifying BRIM connector locations

- installing the EMM-E6 into a Multi Media Access Center (MMAC)

- connecting your device to a network.

NOTE
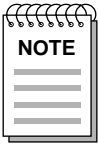
For information on how to install an optional BRIM, refer to your specific BRIM documentation.

3.1 UNPACKING THE EMM-E6

Unpack the EMM-E6 as follows:

Observe all anti-static precautions when handling sensitive electronic equipment.

1. Remove the shipping material covering the EMM-E6.

2. Verify the contents of the packing carton. The carton is shipped with the following items:

Item	Quantity
EMM-E6	1
Firmware Image	1
Grounding Strap	1
RJ45 Adapter Kit	1
Release Notes	1

3. Carefully remove the module from the shipping box. Leave the module in its non-conductive bag until you are ready to install it.

4. Visually inspect the module. If there are any signs of damage, contact Cabletron Systems Technical Support immediately.

5. Place the static grounding strap properly on your wrist before opening the non-conductive bag.

6. Open the non-conductive bag by tearing the black and yellow tape seal.

Do not cut the bag open, as damage to the module could occur.

7. Perform a second visual inspection of the module.

3.2   SETTING MODE SWITCHES

The bank of dip switches located at the top of the EMM-E6 (Figure 3-1) are set to their default positions prior to shipping. Check these switches to ensure that they are in the correct position for normal EMM-E6 operation.
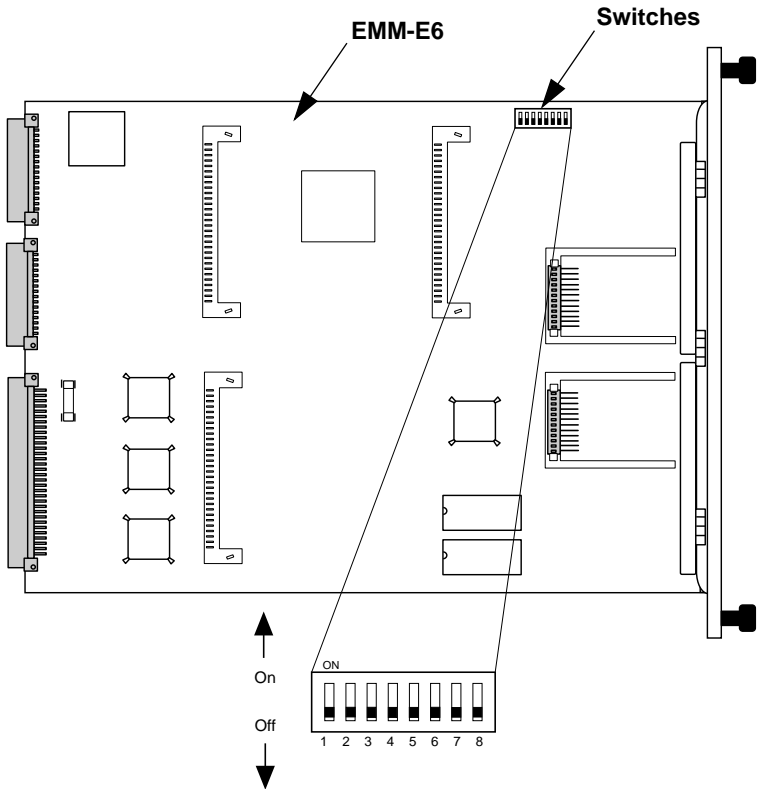
Figure 3-1. EMM-E6 Mode Switches

The potential for electric shock is present inside the MMAC chassis when power is applied. Do not adjust switch settings when the EMM-E6 is within a powered MMAC enclosure. Failure to comply could result in personal injury and/or equipment damage.
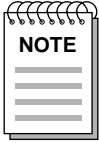
> **NOTE**
>
> *Changes to switch positions only activate their associated functions after the EMM-E6 is reset.*

Switch definitions are as follows:

- Switch 1 - Cabletron Systems use only.

- Switch 2 - Cabletron Systems use only.

- Switch 3 - For manufacturing use only. Keep in **OFF** position.

- Switch 4 - MIMREV (Management Interface Module Revision). This switch remains in the **OFF** position for normal operation. Only if you are using THN-MIM part numbers 9000043-05 and below in your MMAC-FNB should the switch be in the **ON** position.

- Switch 5 - Baud Rate Default. Allows you to set the Console port's baud rate. The **OFF** position sets the baud rate to 9600. The **ON** position sets the baud rate to 2400.

- Switch 6 - Forced Download. Changing the state of this switch (i.e., moving the switch from one position to another) clears download information from NVRAM and forces the EMM-E6 to download an image file from the station acting as the EMM-E6's BOOTP server.
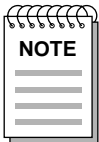
> **NOTE**
>
> *Do NOT change the state of Switch 6 unless you:*
>
> - *have a station acting as a BOOTP server, and that station contains the EMM-E6 image file.*
>
> - *intend to set up a station to act as a BOOTP server for the EMM-E6.*

After changing the state of Switch 6 and repowering the device, the EMM-E6 will request a new image until it either receives the image, or you reset the EMM-E6 again by:

-   using the reset button on the front panel

-   removing the EMM-E6 from the chassis backplane and plugging it back in

-   cycling the MMAC-FNB power.

After resetting the EMM-E6, the device attempts to locate a BOOTP server again. However, the BOOTP request times out after about one minute, and the EMM-E6 boots from FLASH memory.

•   Switch 7 - NVRAM (Non-Volatile Random Access Memory) Reset. The EMM-E6 uses NVRAM to store user entered parameters such the IP address, device name, etc. Changing the state of this switch (i.e., moving the switch from one position to another) and executing a reset of the module resets these parameters to the factory defaults.

Once the EMM-E6 resets, you can either use the defaults or re-enter your own parameters. The EMM-E6 stores these parameters in NVRAM when the device powers down. These parameters remain in NVRAM until the switch changes state again.
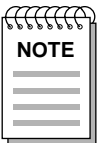
| **NOTE** | *Do not change the state of Switch 7 unless you intend to reset the EMM-E6 user parameters to the factory default settings.* |

•   Switch 8 - Password Defaults. Changing the state of this switch clears user-entered passwords in NVRAM, and restores factory default passwords. Once you reset the EMM-E6, you can use the defaults or re-enter your own passwords.
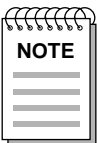
| **NOTE** | *Do not change the state of Switch 8 unless you intend to reset the EMM-E6 user-configured passwords to their factory default settings.* |

3.3   SIMM UPGRADES

The EMM-E6 allows memory upgrades for SDRAM, LDRAM, and
FLASH EEPROM. This section explains how to locate and add or replace
a Single In-line Memory Module (SIMM) for any of these memory types.
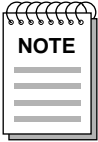
> **NOTE**
>
> *For additional information on SIMMs, or how to upgrade the
> memory in your Module, contact Cabletron Systems
> Technical Support.*

3.3.1   Locating SIMMs

Each memory type has a specific SIMM slot location on the EMM-E6
mother board. When installing SIMM boards, make sure that you place
them in their proper slots. Figure 3-2 illustrates the EMM-E6 SIMM slot
locations and the direction in which to install the SIMMs.
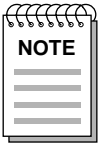
> **NOTE**
>
> *The LDRAM SIMM slot is shipped with an expansion SIMM
> located in it. If you are performing an upgrade to LDRAM,
> ensure that the upgrade SIMM is placed in the proper SIMM
> slot after removing the existing LDRAM SIMM. LDRAM
> SIMM modules placed in the lower SDRAM slot will not
> provide additional main memory. For further information on
> the uses and types of memory in the EMM-E6, please refer to
> Chapter 1.*

Local Dynamic Random Access Memory (LDRAM) SIMM Slot

FLASH Memory SIMM Slot

Direction of Install

EMM-E6

Shared Dynamic Random Access Memory (SDRAM) SIMM Slot
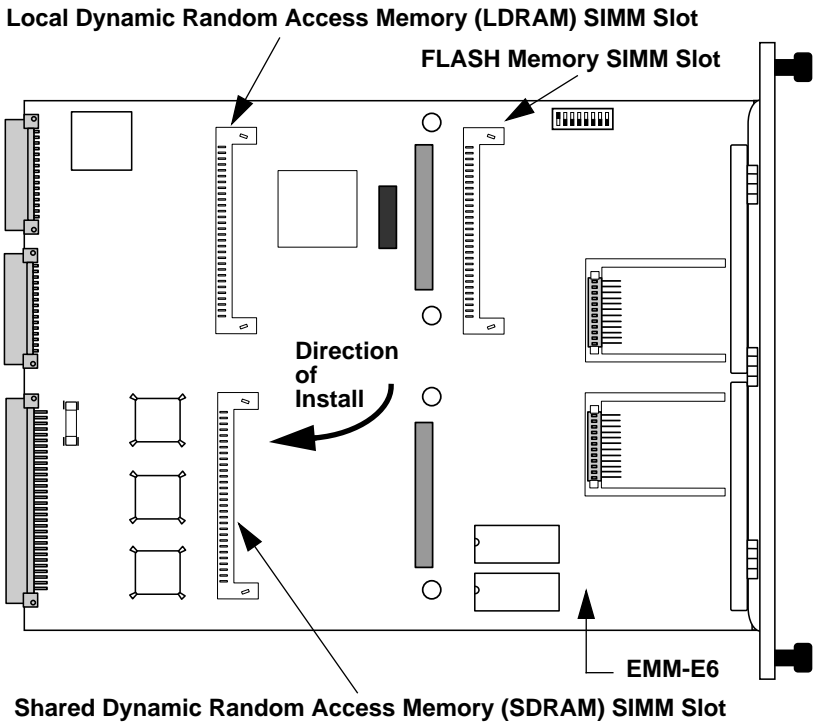
Figure 3-2. SIMM Slot Locations

3.3.2   Installing SIMMs

Installing a SIMM is a simple two step process. After finding the proper SIMM slot location, refer to Figure 3-3 and the following instructions to install your SIMM.
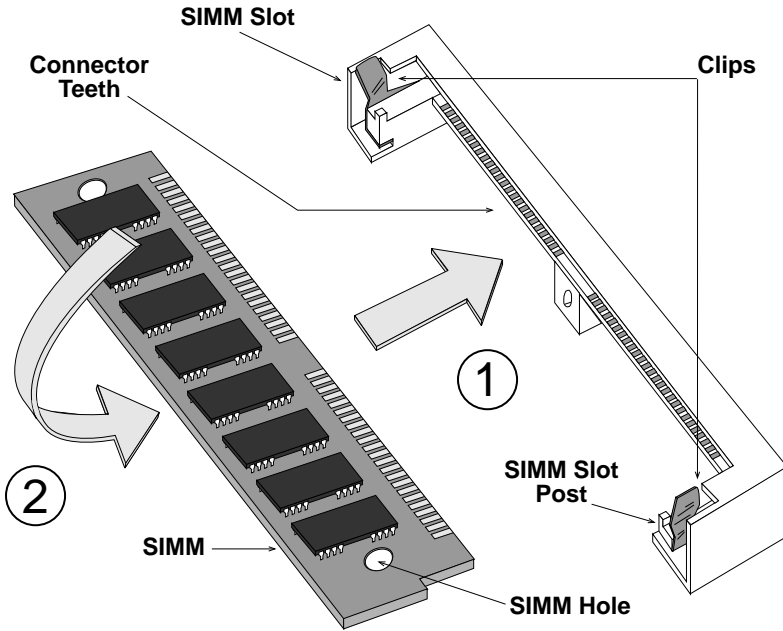
Figure 3-3. Installing a SIMM

To install a SIMM:

> **⚠ CAUTION**
>
> *Observe all anti-static precautions when handling sensitive electronic equipment.*

1.   Insert the SIMM between the connector teeth in the SIMM slot.

2.   Pivot the SIMM back until it locks into the clips in the SIMM slot, and the SIMM holes fit over the SIMM slot posts.

3.4   ADDING/REPLACING EPIMs

This section contains procedures on how to add/replace an Ethernet Port Interface Module (EPIM) to upgrade or change the capabilities of your hub. After installing your new EPIM, refer to appropriate EPIM sections in this chapter to verify proper operation.

Observe all anti-static precautions when handling sensitive electronic equipment.

To install an EPIM:
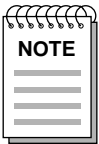
When removing an EPIM, make sure to pull the module straight out so as not to damage the connector.

1. Remove the coverplate or the EPIM (whichever applies).

2. Slide your new EPIM into place, making sure the connectors on the rear of the module and inside the hub attach properly.

3. Install the mounting screw.
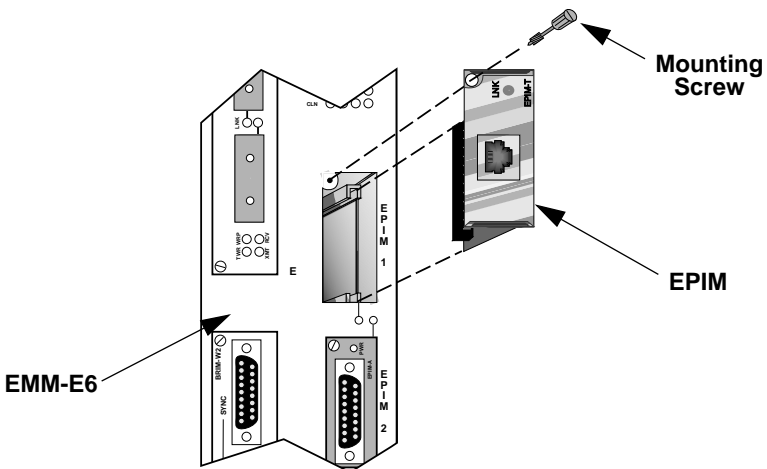
Figure 3-4. Installing an EPIM

3.5 LOCATING BRIMs

This section points out Bridge Router Interface Module (BRIM) connector locations on your EMM-E6 board. Refer to your BRIM Guide for installation procedures and additional information.

The following diagram (Figure 3-5) shows BRIM connector locations for the EMM-E6:
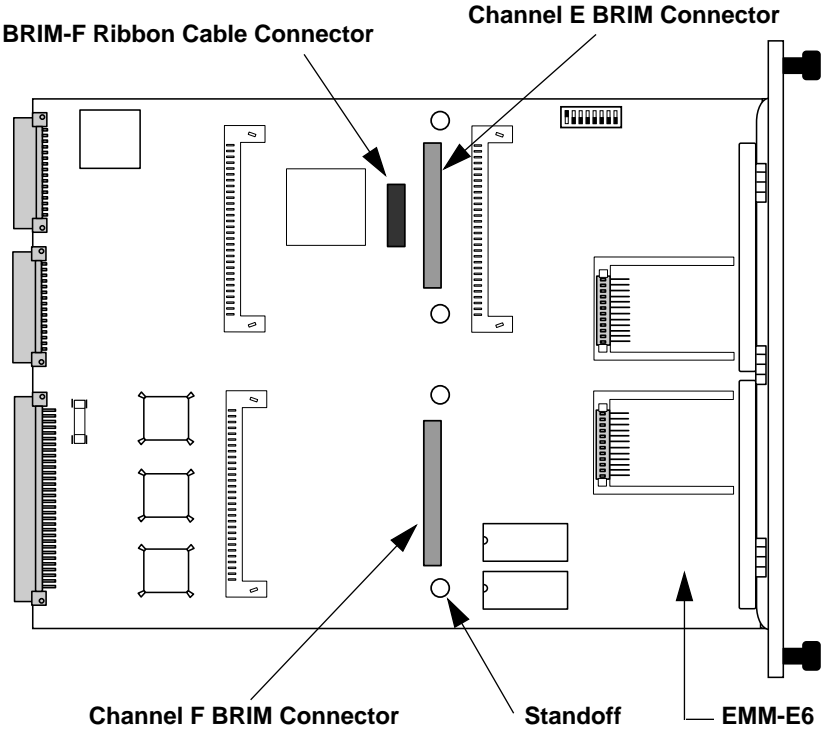
Figure 3-5. BRIM Connector Locations

3.6   PRE-INSTALLATION TEST

Before installing the EMM-E6 in a live network, test the module in a controlled situation to ensure that it is repeating and bridging packets. You can perform this test with two workstations (see Figure 3-6), using an MMAC-FNB, or MMAC-MFNB, installed with an EMM-E6 and a Media Interface Module (MIM) as follows:

1. Install the EMM-E6 and any MIM (e.g., TPMIM, THN-MIM, CXRMIM, FORMIM, etc.) into a non-networked MMAC.

2. Connect the first workstation to an EMM-E6 EPIM or BRIM.

3. Connect the second workstation to the MIM using the appropriate cable or transceiver.

4. Assign the EMM-E6 a valid IP address through Local Management.

5. Designate the first workstation as a file server and the second one as the client (refer to the workstation manuals for establishing one as a file server and one as a client.).

6. Send packets between the two workstations to verify the proper
    operation of the EMM-E6.
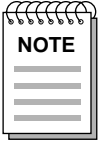
NOTE

*Note: If using UNIX workstations, a "ping" test verifies the
EMM-E6 is operating properly.*

If a failure occurs, refer to Chapter 14, **Troubleshooting**.
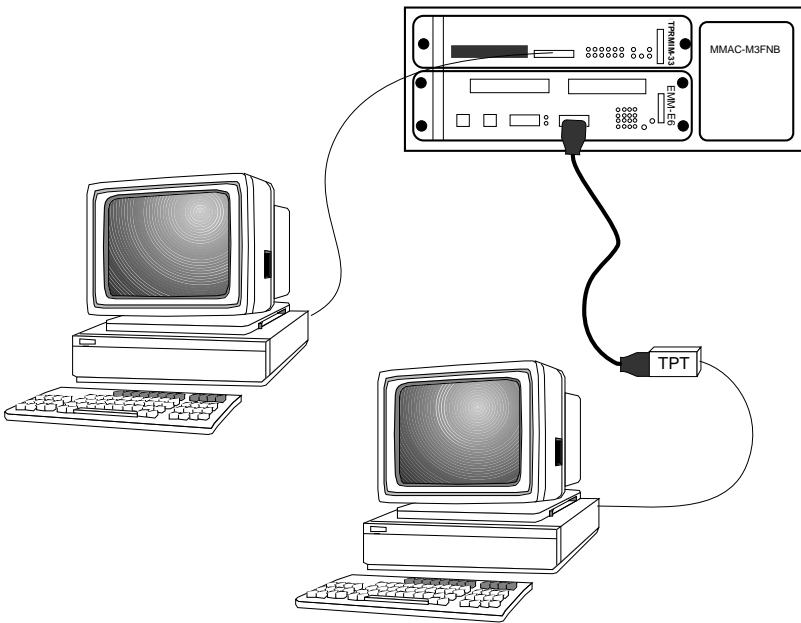
Figure 3-6. Pre-Installation Test

3.7   INSTALLING THE EMM-E6

Installing the EMM-E6 into any MMAC hub is an easy operation and requires no special skills or tools. However, when you install your device, keep the following in mind:

Any installation operations should be performed only by qualified personnel

- You must install the EMM-E6 in slots 1 and 2 (furthest slots to the right) of the MMAC chassis.

- Position RIC MIMs contiguously in any MMAC-FNB series hub, from right to left. This ensures that the channels do not act in a stand-alone manner or desegment from the B or C channel. This does not apply to shunting MMAC-FNBs, where the data path remains unbroken, and allows non-interrupted communication.

Install the EMM-E6 into the MMAC-FNB (backplane) as follows:

NOTE
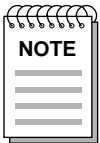
We recommend powering down your MMAC when inserting or removing boards, even though Cabletron Systems modules have "hot swap" capabilities.

1. Remove the safety bars which protect the chassis and remove any module to be replaced or blank MMAC slot covers in accordance with the installation and removal procedures for these items.

2. Holding the EMM-E6 by the edges of the board, align the bottom and top edges of the board with the slot guides. Make sure that both the bottom and top edges of the card rest in the guide slots.

3. Slide the EMM-E6 (Figure 3-7) into slots 1 and 2 (furthest right slots) of the MMAC card cage. Make sure that the module aligns properly in the top and bottom slot guides.

4. Firmly press the module connections into the backplane. Do not try to force the module into place or use the knurled knobs to draw the module into the backplane. Forcing a misaligned module into place can damage the EMM-E6 or the MMAC backplane.
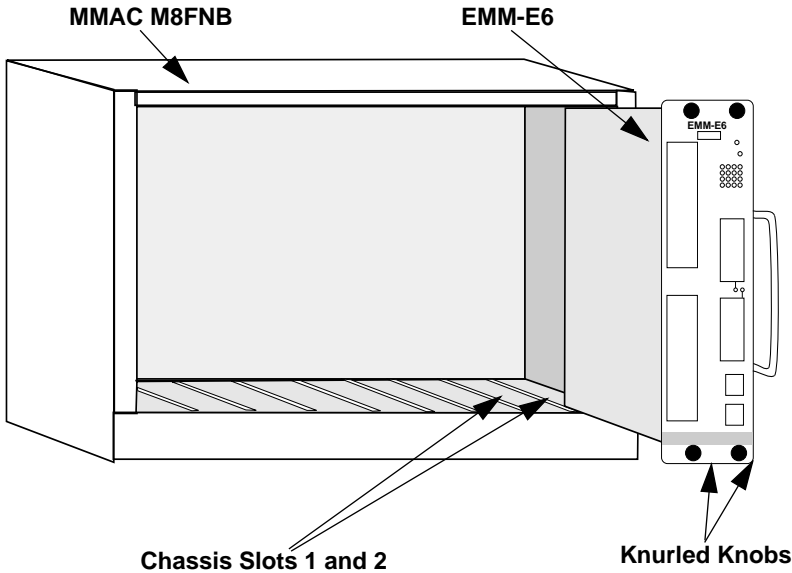
Figure 3-7. Installing the EMM-E6

5. Secure the module to the MMAC chassis by tightening the knurled knobs. If you do not tighten the knurled knobs, vibration can cause the module to lose contact with the backplane and disrupt your network.

7. Re-install the MMAC chassis safety bars.

6. Power-up the MMAC (if it isn't already **ON**).
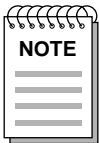
NOTE	*It takes several minutes for the EMM-E6 to boot up. While booting, the EMM-E6 displays boot-up diagnostics on Local Management. Refer to Chapters 4 and 5 for additional information on how to connect and configure a Local Management console.*

7. Observe the status of the LANVIEW LEDs on the EMM-E6. When the CPU LED is flashing, the STBY (standby) LEDs indicate the module's boot state. During this period (up to 5 minutes), the LEDs cycle through a series of internal diagnostics. (See Figure 3-8)
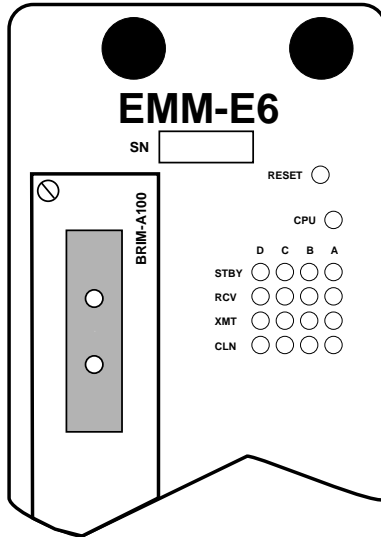
Figure 3-8. EMM-E6 LANVIEW LEDs

8. After the system boot procedure, the LEDs should be in the following conditions:

    • CPU LED flashing, indicating proper EMM-E6 operation.

    • STBY (A, B, C, D) LEDs ON or OFF, depending on the port's position in the Spanning Tree Algorithm.

    • Appropriate EPIM/BRIM LEDs ON (see section 3.9, **Connecting to the Network**, to obtain the appropriate LED status for individual EPIMs; refer to individual **BRIM Guides**).

    • ON LED lit for the active channel D EPIM.

If the LEDs are not operating in the fashion described above, refer immediately to Chapter 14, **Troubleshooting**.

3.8   INSTALLATION CHECK-OUT

After connecting to the network, verify that packets can pass over the network segments via the EMM-E6. Again, you can use two workstations set up as file server and client. Keep the server workstation stationary in the wiring closet with the EMM-E6, and use the client workstation to move to each node connected to the EMM-E6. See Figure 3-9.

1.   After the EMM-E6 is installed in the MMAC, connect the server workstation to either a MIM or to the EMM-E6 via an EPIM or BRIM.

2.   Going to each node connected to the MMAC, connect the client workstation and test the segment.

If a failure occurs, refer to Chapter 14, **Troubleshooting**.
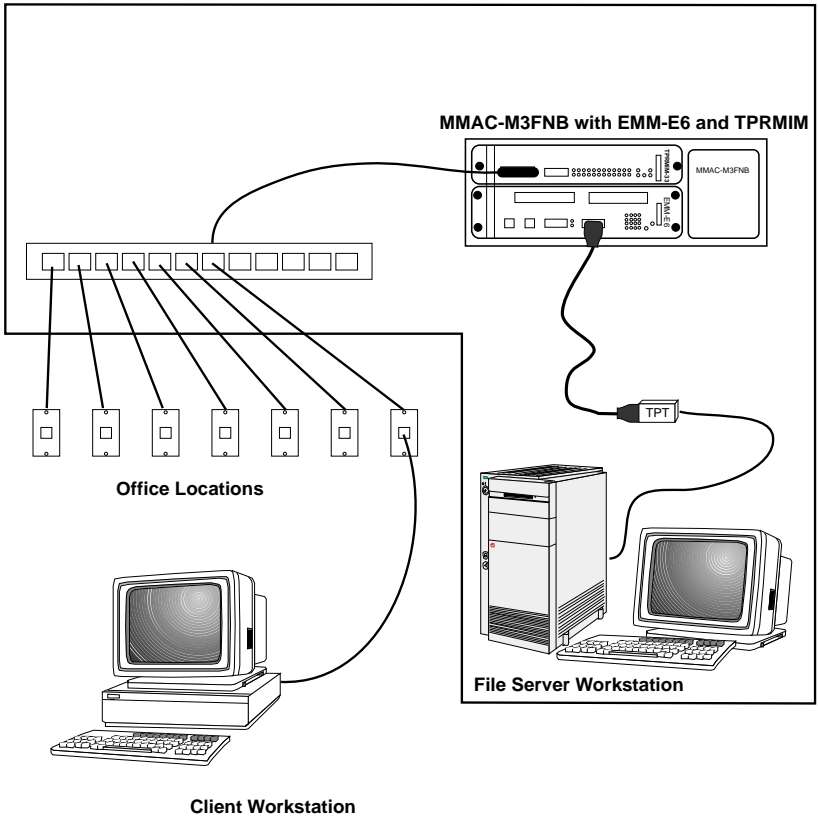
Figure 3-9. Installation Checkout

3.9 CONNECTING TO THE NETWORK

This section gives procedures for connecting the EMM-E6 to the network using the various EPIMs available. When the EMM-E6 is first powered up, the EPIM 1 port acts as the bridge port and the EPIM 2 port is OFF.

Once you have successfully powered up your EMM-E6, you can add network connections. The procedure for connecting Ethernet segments to a hub varies depending on the media and ports you connect. Refer to the following list and perform the procedure described in the subsection(s) that apply to your hub:

- EPIM-T   3.9.1
- EPIM-X   3.9.2
- EPIM-F1,F2,F3   3.9.3
- EPIM-C   3.9.4
- EPIM-A   3.9.5

3.9.1 Connecting a Twisted Pair Segment to an EPIM-T

Before connecting a segment to the EPIM-T, check each end of the segment to determine wire cross-over. If the wires do not cross over, use the switch on the EPIM-T to internally cross over the RJ45 port. Refer to Figure 3-10 to properly set the EPIM-T cross-over switch.

NOTE
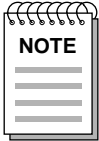
To establish link, you must have an odd number of cross-overs (preferably one) between 10BASE-T devices of the same type (i.e., from repeater to repeater or transceiver to transceiver).

Position X
(crossed over)

1. RX+	5. NC
2. RX-	6. TX-
3. TX+	7. NC
4. NC	8. NC

Position =
(not crossed over)

1. TX+	5. NC
2. TX-	6. RX-
3. RX+	7. NC
4. NC	8. NC
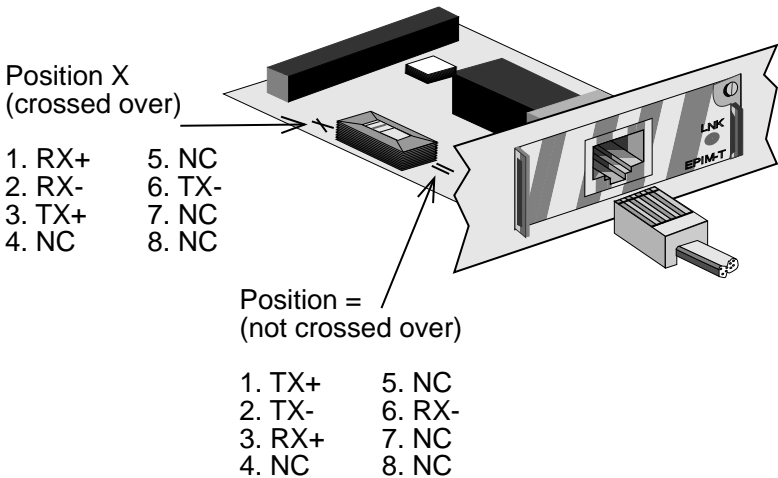
Figure 3-10. EPIM-T Cross-over Switch

To connect an EPIM-T to a Twisted Pair Segment:

1. 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. (See Figure 3-10.)

2. Check that the **LNK** LED for the port is on. If the LED is not on, perform each of the following steps until it is:

   a. Check that the 10BASE-T device at the other end of the twisted pair segment is powered.

   b. Verify that the RJ45 connectors on the twisted pair segment have the proper pinouts (Figure 3-11).

   c. Check the cable for continuity.

   d. Check that the twisted pair connection meets dB loss and cable specifications outlined in 10BASE-T Twisted Pair Network Requirements (Chapter 2).
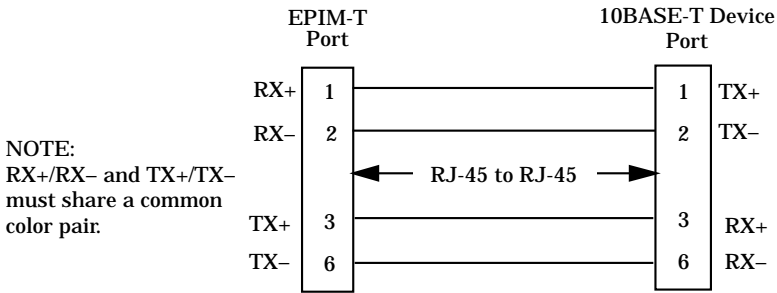
Figure 3-11. Cable Pinouts - EPIM-T RJ45 Port

If you still cannot establish link, contact Cabletron Technical Support.

3.9.2   Connecting an AUI Cable to an EPIM-X
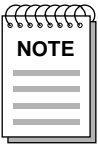
> **NOTE**
>
> *The Signal Quality Error (SQE) switch remains in the OFF position for most network connections. However, some Data Terminal Equipment (DTE) requires SQE. Refer to your DTE manual for SQE requirement information.*

To connect an EPIM-X to a device not requiring SQE:

1.   Verify that the **SQE** LED on the EPIM-X is off. If the **SQE** LED is on, set the position of the SQE switch to off.
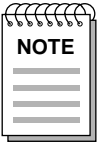
> **NOTE**
>
> *If the SQE light remains on, even though the SQE switch is in the OFF position, contact Cabletron Technical Support.*

2.   Attach one end of an AUI cable, no longer than 50 meters in length, to the port located on the EPIM-X (Figure 3-12) and the other end to the intended node.

ON Position
(Toward Back
of EPIM)

OFF Position
(Toward Front
of EPIM)
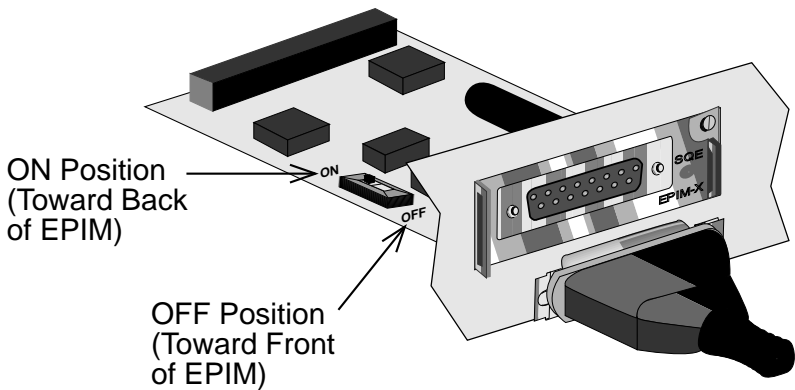
Figure 3-12.   The EPIM-X

3.9.3 Connecting to an EPIM-F1/F2, or EPIM-F3

When connecting a fiber optic link segment to an EPIM-F1/F2, or EPIM-F3 keep the following in mind:

- When connecting a fiber optic link segment with SMA 906 connectors to an EPIM-F1 with SMA ports, make sure each connector uses half alignment, NOT full alignment, sleeves.

NOTE
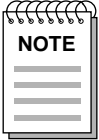
A full alignment sleeve damages the receive port. SMA 905 connectors do not need alignment sleeves.

- When connecting a fiber optic link segment with ST connectors to an EPIM-F2 with ST ports, keep in mind that ST connectors attach to ST ports much like BNC connectors attach to BNC ports. Insert the connector into the port with the alignment key on the connector inserted into the alignment slot on the port. Turn the connector to lock it down.

- The physical communication link consists of two strands of fiber optic cabling: the Transmit (TX) and the Receive (RX). The Transmit strand from a module port connects to the Receive port of a fiber optic Ethernet device at the other end of the segment (i.e., TX of the applicable port on the module goes to RX of the other fiber optic device). The Receive strand of the applicable port on the module connects to the Transmit port of the fiber optic Ethernet device (i.e., RX of the applicable port on the module goes to TX of the other fiber optic device).

We recommend that you label the fiber optic cables to indicate Receive and Transmit ends. Cabletron Systems prelabels its cable. At one end of the cable, one fiber is labeled 1, and the other fiber is labeled 2. This pattern repeats at the other end of the cable. If you did not purchase your cable from Cabletron Systems, be sure to label your cable in this manner.

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

To connect a fiber optic link segment to an EPIM-F1/F2 or an EPIM-F3:

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 on each fiber strand.

2. On the EMM-E6, attach the fiber labeled 1 to the applicable receive port, labeled RX (Figure 3-13).

3. On the EMM-E6, attach the fiber labeled 2 to the applicable transmit port, labeled TX.

4. At the other end of the fiber optic cable, attach the fiber labeled 1 to the transmit port of the device and the fiber labeled 2 to the receive port.
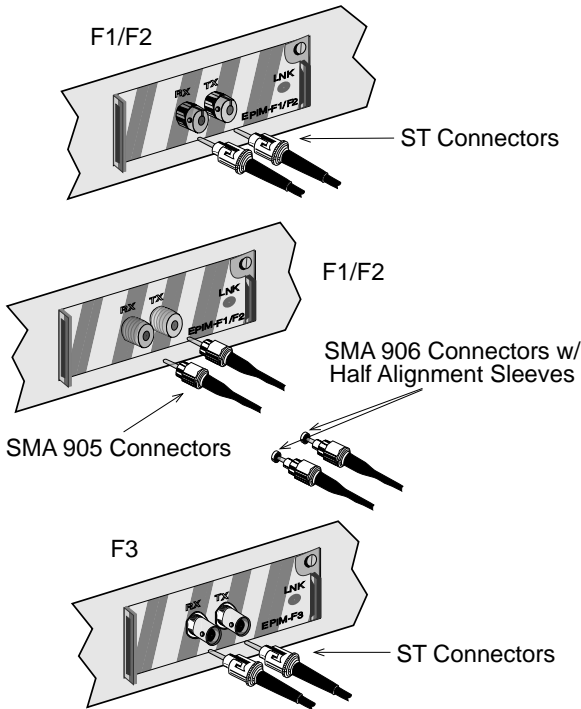
Figure 3-13. The EPIM-F1/F2 and EPIM-F3

5.   Check that the **LNK** LED on the applicable module port is on. If the
     LED is not on, perform each of the following steps until it is:

     a.   Check that the device at the other end of the link is powered.

     b.   Verify proper "cross-over" of fiber strands between the applicable
          port on the module 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 Fiber Optic Network Requirements (Chapter 2).

If you still cannot establish link, contact Cabletron Technical Support.

3.9.4   Connecting a Thin-Net Segment to an EPIM-C

To connect a thin-net segment to an EPIM-C:

1.   Set the Internal Termination Switch (Figure 3-14), located above the port (when the EPIM has been inserted into the EMM-E6) and labeled TERM to:

   • the **ON** position (●) to internally terminate the thin-net segment at the port.

   • the **OFF** position (○) if you do not want the thin-net segment to internally terminate at the port.

2.   If the Internal Termination Switch is in the **On** position, connect the thin-net segment directly to the BNC port.

3.   If the Internal Termination switch is in the **Off** position:

   a.   Attach a BNC T-connector to the BNC port on the module.

   b.   Attach the thin-net segment to one (1) of the female connectors on the T-connector.

   ⚠ **CAUTION**
   Failure to terminate each T-connector segment may result in improper segment operation. Place a terminator on any open female connection on the T-connector.

   c.   Attach another thin-coaxial segment or a terminator to the other female connector on the T-connector.

   Connecting a thin-net segment to earth ground at more than one point could produce dangerous ground currents.

When internal termination switch
is set to off (○):

Connect BNC T-connector to port.

Attach a terminator or terminated
thin-net segment to one female
connector of tee-connector.

Connect a terminated thin-net
segment to other female connector
of T-connector.
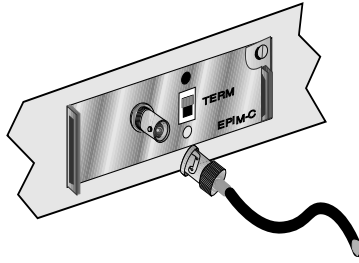
Attach thin-net segment directly to BNC
connector when internal termination
switch is set to on (●).
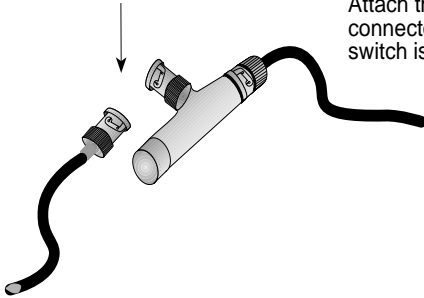
Figure 3-14. The EPIM-C

3.9.5 Connecting an AUI Cable to an EPIM-A

NOTE
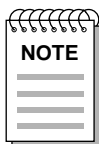
Ensure that the external transceiver to which you connect the EPIM-A does not have the Signal Quality Error (SQE or "heartbeat") test function enabled. The EPIM does not operate if the transceiver has the SQE test function enabled. Refer to the applicable transceiver manual for additional information.

To connect an EPIM-A to an external network segment:

1. Check that the **PWR** LED on the EPIM-A is on. If the **PWR** LED is not on, contact Cabletron Systems Technical Support.

2. Attach an external transceiver to the network segment intended for AUI port connection. For additional information, refer to the applicable transceiver manual.

3. Attach an AUI cable, no longer than 50 meters in length, to the transceiver you connected to the network in step 2.

4. Connect the AUI cable to the AUI port located on the EPIM-A. (See Figure 3-15.)
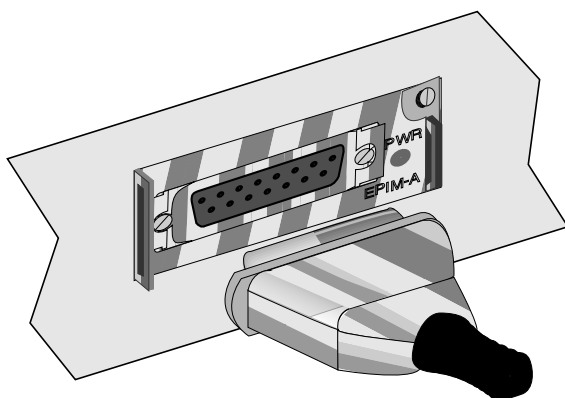
Figure 3-15. The EPIM-A

5. Lock the AUI connector into place using the connector slide latch.

6. If the transceiver **PWR** LED is off with the AUI cable connected:

   a. Check the AUI connections for proper pinouts. Appendix A lists the pinouts for the transceiver connection.

   b. Check the cable for continuity.

   c. Reconnect the AUI cable to the EMM-E6 and the device.

If the transceiver **PWR** LED remains off, contact Cabletron Systems Technical Support.

CHAPTER 4

ATTACHING A CONSOLE

This chapter describes how to attach a Local Management console to the EMM-E6, and lists the setup and configuration requirements for:

- console/terminal
- console cable
- console cable connections.

4.1 CONFIGURING YOUR TERMINAL

The following instructions outline how to configure your console (terminal) to communicate with Local Management. Refer to your specific terminal manual for more instructions if necessary.

To access Local Management for the EMM-E6, you need either:

- a VT200 or VT300 series terminal
- a PC emulating a VT200 or VT300 series terminal.

To access the Setup Directory on a VT series terminal, press **F3**. The following table lists the required terminal setup for a VT series terminal.

Table 4-1. 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................................	->	VT300, 7 Bit Controls
ID number	->	VT320ID or VT100ID
Cursor Keys	->	Normal Cursor Keys
Power Supply	->	UPSS DEC Supplemental
Communications Setup Menu		
Transmit	->	Transmit=9600
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 Set-up Menu		
Keys.................................	->	Typewriter Keys
Auto Repeat	->	any option
Keyclick	->	any option
Margin Bell.......................	->	Margin Bell
Warning Bell	->	Warning Bell

4.2   CONFIGURING A CONSOLE CABLE

This section outlines the proper cable configurations for connecting the EMM-E6 to a Local Management terminal. For information on the appropriate pinouts, refer to Appendix A of this User's Guide.

You need the following hardware (supplied with your EMM-E6) to connect the EMM-E6 to a terminal:

- an RS232 cable
- an adapter
- a device cable

The adapter you use depends on whether you connect to LM from a VT series terminal, or a VT-emulating PC. Read the information included with the cable kit to make sure you are using the right adapter.

To configure the cables:

1.   Plug a straight-through twisted pair cable (e.g., an RS232 cable) into the EMM-E6 RJ45 COM 2 Port.
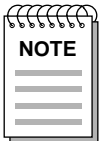
> **NOTE**
>
> *Do not attempt to utilize the COM 1 port for Local Management, as the COM 1 port is intended to be used for monitoring an Uninterruptible Power Supply (UPS). The method for configuring the COM 1 port for this purpose is described later in this chapter.*

2.   Plug the other end of the RS232 cable into the adapter.

3.   Connect the adapter into the device cable and plug the other end of the device cable into the terminal or terminal emulator. Detailed descriptions of this process for VT terminals or terminal-emulating PCs follow.

4.2.1 Connecting to a VT Series Terminal

To connect a VT Series terminal to a Cabletron module Console port (Figure 4-1):

1. Connect the RJ45 connector at one end of the cable to the Console port on the Cabletron module.

2. Plug the RJ45 connector at the other end of the cable into the RJ45 to DB25 female adapter.

3. Connect the DB25 adapter to the port labeled COMM on the VT terminal.
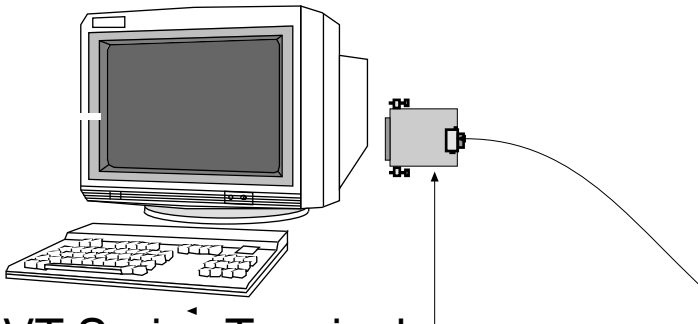
Figure 4-1. Connecting a VT Series Terminal

4. Turn on the terminal and access the Setup Directory. Follow the directions in the previous section and set up your VT terminal to match the configuration given in Table 4-1.

5. When these parameters are set, the Local Management password screen will appear. Refer to Chapter 5, Accessing Local Management.

4.2.2   Connecting to an IBM PC or Compatible

To connect an IBM PC or compatible running VT terminal emulation to a Cabletron module Console port (Figure 4-2):

1.   Connect the RJ45 connector at one end of the cable to the Console port on the Cabletron module.

2.   Plug the RJ45 connector at the other end of the cable into the RJ45 to DB9 adapter.

3.   Connect the DB9 adapter to the communications port on the PC.
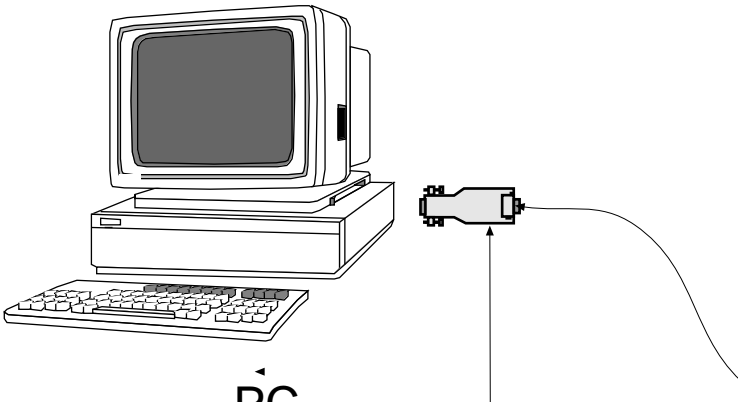
Figure 4-2. Connecting an IBM PC or Compatible

4.   Turn on the PC and configure your VT emulation package to match the configuration given in Table 4-1.

5.   When these parameters are set, the Local Management password screen will appear. Refer to Chapter 5, Accessing Local Management.

4.3   PINOUT DESCRIPTIONS

Table 4-2. RJ45 to DB9 Adapter (PC Adapter):

RJ45		DB9	
Pin	**Color**	**Pin**	**Description**
1	Blue	2	Receive
4	Red	3	Transmit
5	Green	5	Ground
2	Orange	7	Send Request
6	Yellow	8	Clear to Send

Table 4-3. RJ45 to DB25 Adapter (VT Series Adapter):

RJ45		DB25	
Pin	**Color**	**Pin**	**Description**
4	Red	2	Transmit
1	Blue	3	Receive
6	Yellow	5	Clear to Send
5	Green	7	Ground
2	Orange	20	Terminal Ready

4.4   CONFIGURING A UPS CABLE

To configure an Uninterruptible Power Supply (UPS) cable:

1. Plug a straight-through twisted pair, RS232, cable into the EMM-E6 RJ45 COM 1 Port.

2. Plug the other end of the RS232 cable into the adapter (PN 9372066) and connect the adapter to the UPS.

3. Set COM 1 in the LM Configuration screen to UPS. Refer to Chapter 7, **Configuration Screen**, for additional information regarding UPS connection.

CHAPTER 5

ACCESSING LOCAL MANAGEMENT

With your terminal properly configured, and the correct physical cable connections in place, you can access the Local Management interface.

To access Local Management:

1. Turn the terminal on, and press the **Return** key. The EMM-E6 Password Screen, Figure 5-1, appears.

```
                    EMM-E6-960 LOCAL MANAGEMENT
                    Cabletron EMM-E6 Revision 0.00.00


                    Cabletron Systems Incorporated
                    35 Industrial Way, P.O. Box 5005
                    Rochester, NH  03867-0505  U.S.A.
                            (603) 332-9400


           (c) Copyright Cabletron Systems, Inc.  1994


                    EMM-E6-960 F/W Version:   0.00.00

                       Boot PROM Version:  00.00.00
                    EMM-E6-960 Board Rev#:  00.00.00



         Enter USER PASSWORD: ████████████████████████
```

Figure 5-1. EMM-E6 Password Screen

2. Enter your **Password** and press **Return**. The default Super-User access password is the **Return** key (which defaults internally to 'public').
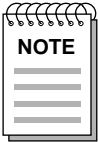
> **NOTE**
>
> *Your password is one of the community names specified in the Community Name Table. Access to certain LM capabilities depends on the degree of access accorded that community name. See Chapter 6,* **Community Names***, for additional information.*

*   If you enter an invalid password, the EMM-E6 ignores the entry, and the cursor returns to the beginning of the password entry field.

*   After entering a valid password, an associated access level flashes across the bottom of the screen, and then the Feature Selection Screen, Figure 5-2, appears.
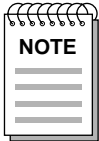
> **NOTE**
>
> *Entering 10 incorrect passwords in a row causes an access violation. In such an event, the EMM-E6 disconnects from the network and requires a reset to continue operation.*

EMM-E6-960 LOCAL MANAGEMENT
Cabletron EMM-E6 Revision 0.00.00
FEATURE SELECTION

    F6   COMMUNITY NAME TABLE
    F7   IP ADDRESS ASSIGNMENT
    F8   COMPONENT TRAP TABLE
    F9   SNMP TOOL SUPPORT
    F10   MIB NAVIGATOR
    F14   ROUTER SETUP

          DEVICE STATISTICS

          EXIT LIM SERVICE
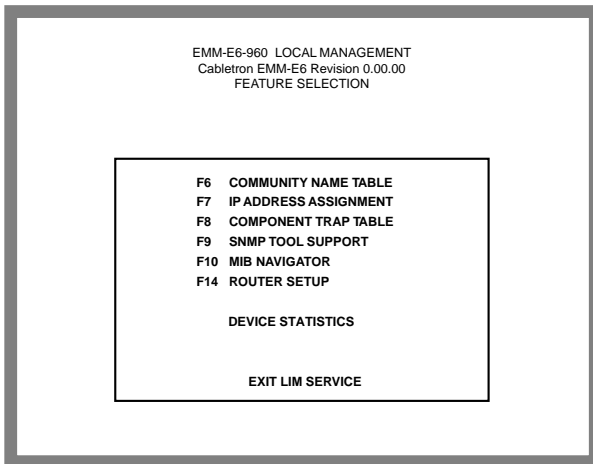
Figure 5-2. Feature Selection Screen

3. Use the arrow keys to highlight an option, and press **Return** (or simply use the corresponding Function key). The selected screen appears.

If you do nothing on LM for 15 minutes, the Password Screen reappears. At this point, you must re-enter the password to continue using EMM-E6 Local Management.

CHAPTER 6

COMMUNITY NAMES

The Community Name Table option lets you set Local Management community names. These names act as passwords to LM and provide security for your EMM-E6. You can control EMM-E6 access by establishing up to four different levels of security authorization - basic read-only, read-only, read-write, and super-user.

Super-user access gives you full management privileges and allows you to change existing passwords and edit all modifiable MIB objects for the EMM-E6 and additional Bridge/Router Interface Modules (BRIMs).

6.1 ACCESSING THE COMMUNITY NAME TABLE

To access the Community Name Table Screen:

1. From the Feature Selection Screen, use the arrow keys to highlight the **Community Name Table** option, and press the **Return** key. The Community Name Table Screen, Figure 6-1, appears.

```
              EMM-E6-960  LOCAL MANAGEMENT
              Cabletron EMM-E6 Revision 0.00.00
                 COMMUNITY NAME TABLE

    <<    PASSWORD AUTHORIZATION = SUPER-USER    >>

            NOTE:  S/U names are LOCAL passwords


       Community Name                    Access


          public                     BASIC-READ
          public                     READ-ONLY
          public                     READ-WRITE
          public                     SUPER-USER




 SAVE      IP TABLE      TRAP TABLE    SNMP TOOLS    CLI     RETURN
  F6         F7             F8            F9         F10
```

Figure 6-1. Community Name Table Screen

6.2 COMMUNITY NAME TABLE SCREEN FIELDS

This section briefly explains each Community Name Table Screen field.

Community Name
Displays the community name through which a user can access LM. All community names act as passwords to Local Management. Depending on the assigned access, community names can vary in privileges.

Access
Indicates the privileges accorded each community name. Possible selections are:

BASIC-READ	The community name corresponding to this status has limited read-only access to the EMM-E6 and does not include access to security protected fields requiring a higher-level of authorization (read-only, read-write, or super-user).
READ-ONLY	This allows for extended read-only access to EMM-E6/LM fields, and excludes access to security protected fields of read-write or super-user authorization.
READ-WRITE	This allows you to read and write to EMM-E6/LM fields, excluding fields security protected for super-user access only.
SUPER-USER	This access status gives the user read-write access to the EMM-E6/LM and allows changes to be made to all modifiable parameters including: community names, IP addresses, traps, and SNMP objects.

6.3 ESTABLISHING COMMUNITY NAMES

In order for any Community Name Table edits to take effect, you must have super-user access. In other words, when you log into LM, you must do so with a super-user password. A password from any of the other levels of access (basic-read, read-only, or read-write) does not allow you to edit the Community Name Table Screen.
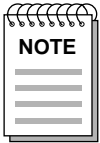
> **NOTE**
>
> *Any community name assigned in the Community Name Table is a password to its corresponding level of LM access. These names are case sensitive. The community name assigned super-user access is the only one that gives you complete access to LM. **Remember this name.***

Establishing community names:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the access level of your choice.

2. Enter the name into the field (maximum 32 characters).

3. Press the **Return** key.

4. Repeat **steps 1 - 3** to modify any other community names.

5. Use the arrow keys to highlight the **Save** command at the bottom of the screen and press the **Return** key. The message "SAVED OK" appears. The EMM-E6 saves the community names in memory, and implements their access modes.

    If you exit without saving, a "NOT SAVED?" message appears above the SAVE command. If you proceed to exit without saving, you lose all edits.

6. To exit the screen use the arrow keys to highlight **Return** and then press the **Return** key. The Feature Selection Screen appears.

CHAPTER 7

CONFIGURATION SCREEN
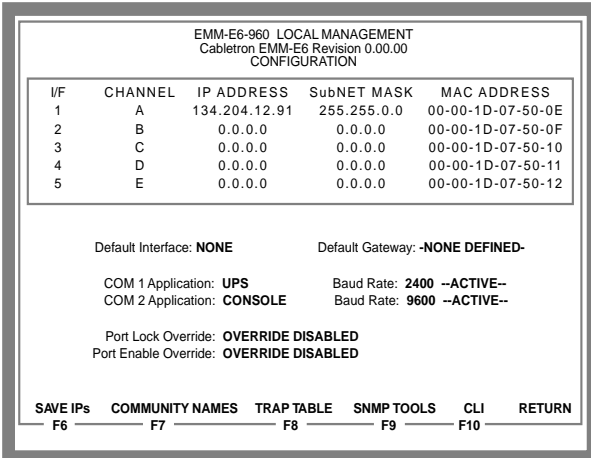
In the EMM-E6 Configuration Screen you can assign an IP address and Subnet Mask to the EMM-E6. You can also:

- set the Default Interface
- set the Default Gateway
- override locked ports
- enable all ports.

7.1 ACCESSING THE CONFIGURATION SCREEN

To access the Configuration Screen:

1. From the Features Selection Screen, use the arrow keys to highlight the **IP Address Assignment** option, and press the **Return** key. The Configuration Screen, Figure 7-1, appears.

```
                    EMM-E6-960  LOCAL MANAGEMENT
                    Cabletron EMM-E6 Revision 0.00.00
                            CONFIGURATION

  I/F     CHANNEL    IP ADDRESS    SubNET MASK     MAC ADDRESS
   1        A      134.204.12.91   255.255.0.0   00-00-1D-07-50-0E
   2        B          0.0.0.0        0.0.0.0    00-00-1D-07-50-0F
   3        C          0.0.0.0        0.0.0.0    00-00-1D-07-50-10
   4        D          0.0.0.0        0.0.0.0    00-00-1D-07-50-11
   5        E          0.0.0.0        0.0.0.0    00-00-1D-07-50-12


      Default Interface: NONE        Default Gateway: -NONE DEFINED-

      COM 1 Application: UPS          Baud Rate: 2400 --ACTIVE--
      COM 2 Application: CONSOLE      Baud Rate: 9600 --ACTIVE--

      Port Lock Override: OVERRIDE DISABLED
      Port Enable Override: OVERRIDE DISABLED


  SAVE IPs   COMMUNITY NAMES   TRAP TABLE   SNMP TOOLS   CLI      RETURN
  — F6 ———————— F7 ——————————— F8 ————————— F9 ———————— F10 —
```

Figure 7-1. Configuration Screen

7.2 CONFIGURATION SCREEN FIELDS

The following briefly explains each Configuration Screen field.

I/F
Displays the interface number (1 to 6) corresponding to a particular
EMM-E6 channel. This number allows the EMM-E6 to accurately
identify MIB II channel information. The following table illustrates the
I/F number to channel association.

I/F	Channel
1	A
2	B
3	C
4	D
5	E
6	F

Channel A is the original Ethernet bus channel. Channels B & C are the
Flexible Network Bus (FNB) channels. Channel D is an external Ethernet
network accessed through an Ethernet Port Interface Module (EPIM).
Channels E and F are external connections through optional BRIMs.
Refer to Chapter 1 of this User's Guide for a more complete description
of channels.
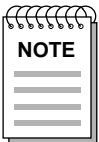
> **NOTE**
>
> *Channel E and F configuration options are dynamic. This
> means the EMM-E6 only provides options for Channels E or
> F if you have a BRIM module installed in one of these slots.*

IP Address
Displays the IP address for each interface of the EMM-E6. This IP
address will be used for the sending and receiving of SNMP data and
should be configured for the interface with a connection to the network
management station. If the network management station is located on a
different network or subnet, the Default Interface and Default Gateway
must be properly configured to allow the proper functioning of SNMP
management.

SubNET Mask
Displays the Subnet Mask for each of the six EMM-E6 channels in dotted decimal notation.

MAC Address
Displays the physical address of each bridge interface.

Default Interface
Displays the default interface number for the EMM-E6 default gateway. This field defaults to NONE.

Default Gateway
Displays the default gateway for the EMM-E6. You cannot use this field until you enter an appropriate value for the Default Interface.

COM 1 Application
Displays a port application setting of OFFLINE, UPS, or SLIP.

COM 2 Application
Displays a port application setting of CONSOLE.

Baud Rate
Displays the Baud Rate setting of the device attached to the EMM-E6 through that COM port. The setting for COM 1 is 2400 or N/A; the setting for COM 2 is 9600.

Port LOCK Override
This command overrides the port locking security feature, and unlocks all ports in the MMAC containing the EMM-E6.

Port ENABLE Override
This command overrides the Port Disable feature, and enables all ports in the MMAC containing the EMM-E6.

7.3 SETTING THE HOST IP ADDRESS

The table on the Configuration screen allows you to assign an IP address and Subnet Mask to the EMM-E6.
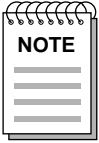
> **NOTE**
>
> *The Host IP applies to each interface.*

To set the Host IP:

1. Use the arrow keys to highlight the **IP Address** field.

2. Enter the IP address into this field. The format for this entry is XXX.XXX.XXX.XXX, with values for XXX ranging from 0 to 254. The EMM-E6 rejects non-numerics, adjacent dots (periods), or an entry without dots separating the four XXX values.

3. Press the **Return** key. The screen displays the Host IP address and changes any existing Subnet Mask to the default Subnet Mask for the IP address entered.

4. Use the arrow keys to highlight the SAVE IPs command.

5. Press the **Return** Key. At the resulting prompt, typing "Y" will cause the EMM-E6 to reset and load the Host IP changes into NVRAM.
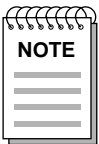
> **NOTE**
>
> *It takes approximately 35 seconds for the EMM-E6 to save and reset. The board is inoperable during this time. After the EMM-E6 resets, the password screen appears and you must re-enter Local Management.*

If you exit the Configuration Screen without saving, you lose all edits.

7.4   MODIFYING A SUBNET MASK

NOTE
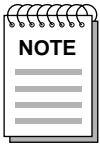
Consult your Network Administrator prior to modifying any of the natural Subnet Masks.

The EMM-E6 automatically enters the natural Subnet Mask for any IP address that you enter. A natural Subnet Mask is a logical separation between network and host identifiers within the IP address. The EMM-E6 allows you to modify this mask to best suit your needs.

The Subnet Mask defines how your EMM-E6 treats SNMP trap IP destination addresses in its Trap table (see Chapter 8, **Trap Table Screen**, for additional information on traps).

Using the Subnet Mask, the EMM-E6 logically determines one of two possible locations, either **on** or **not on** its own subnet, for each trap IP destination address in its trap table. If the address is **on** its own subnet, the EMM-E6 transmits directly to the workstation with that address. If the address is **not on** its subnet, the EMM-E6 transmits to the workstation with that IP address combined with the default gateway router MAC address.

Use the natural Subnet Mask when:

- workstations in the Trap table reside on a different subnet (i.e., across a gateway or external router), and you want these workstations to receive SNMP traps

- the EMM-E6 provides a natural subnet mask that fits your host/ network identifier scheme.

Modify the natural Subnet Mask when:

- workstations in the Trap table reside on a different subnet (i.e., across a gateway or external router), and you want these workstations to receive SNMP traps

- the EMM-E6 does NOT provide a natural Subnet Mask that fits your host/network identifier scheme.
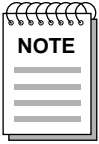
NOTE	*Make sure to modify the Subnet Mask option in conjunction with the Default Gateway option.*

To modify the Subnet Mask:

1. Use the arrow keys to highlight the appropriate **Subnet Mask** field.

2. Enter the **Subnet Mask** in this field in the format of XXX.XXX.XXX.XXX, with XXX ranging from 0 to 255.

3. Press the **Return** key.

4. Repeat **steps 1 - 3** for each interface you want to modify.

The IP Address Table now contains Subnet Mask information specific to your network.

7.5 SETTING DEFAULT GATEWAY AND INTERFACE

The Default Gateway is the IP address of the network connection (i.e., gateway or another external router) used in forwarding management information from the EMM-E6 (e.g., SNMP traps) to a network management station.

The Default Interface is the channel that the EMM-E6 uses to access the Default Gateway. Make sure to set the Default interface to reflect the correct interface channel for the Default Gateway.
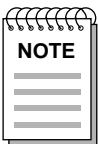
NOTE	*The Default Gateway field will not allow itself to be modified until a Default Interface has been correctly configured on the EMM-E6.*

To set the Default Gateway and its associated Default Interface:

1. Use the arrow keys to highlight the **Default Interface** field.

2. Enter the interface number of the EMM-E6 for the Default Gateway in this field. The interface number will be a value between 1 and 6. A table of the interface numbers may be found in section 7.2.
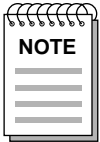
> **NOTE**
>
> *The EMM-E6 will not allow Local Management to configure the Default Interface to utilize an unsubscribed interface. For example: To select Interface 5 as the Default Interface, a BRIM module must first be configured to the E channel of the EMM-E6.*

3. Press the **Return** key. If the EMM-E6 accepts your entry as a valid Default Interface, it displays "Previous Default Interface Marked Invalid" at the top of the screen.

4. Use the arrow keys to highlight the **Default Gateway** field.

5. Enter the gateway's IP address in this field. The format for this entry is XXX.XXX.XXX.XXX with values for XXX ranging from 0 to 254.

6. Press the **Return** key. If the EMM-E6 accepts your entry as a valid Default Interface, it displays "Previous Default Interface Marked Invalid" at the top of the screen.

You have now established a Default Gateway and Default Interface for your EMM-E6.

7.6 CONNECTING/DISCONNECTING A UPS

The EMM-E6 provides the option of connecting to an Uninterruptible Power Supply (UPS) using Local Management.

To enable the UPS connection using EMM-E6/LM:

1. Use the arrow keys to highlight the **COM 1 Application:** field.

2. Press the **Return** key until "UPS" appears in the field. This field toggles between "OFFLINE", which is the default value, "UPS", and "SLIP".

3. Use the arrow keys to highlight the COM 1 **Baud Rate** field.

4. Press the **Return** key until "2400 Connect?" appears in the field.

5. Use the arrow keys to highlight **Connect?**.

6. Press the **Return** key. The request "Y/N:_" appears.

7. Enter **Y** if you want to connect a UPS, or **N** if you do not want a UPS connection. Entering a **Y** response connects the EMM-E6 to the UPS and "**-- Active --**" appears in the **Connect?** field.

8. Press the **Return** key.

To disable the UPS connection using EMM-E6/LM:

1. Use the arrow keys to highlight **-- Active --** in the COM 1 field.

2. Press the **Return** key. The option "**Disconnect? Y/N:**" appears.

3. Enter **Y** if you want to disconnect a UPS, or **N** if you want to remain connected. Entering a **Y** response disconnects the EMM-E6 from the UPS. "**-N/A-**" will appear in the **Baud Rate** field, and the COM1 Application field changes to "OFFLINE".

4. Press the **Return** key.

7.7   UNLOCKING PORTS

When you lock the chassis for security reasons (e.g., using remote inband management), unauthorized devices cannot communicate through an MMAC-FNB chassis station port. The Port LOCK Override function provides fail-safe recovery if you cannot unlock ports using remote inband SNMP.

To use the Port LOCK Override:

1.   Use the arrow keys to highlight the **Port LOCK Override** field.

2.   Press the **Return** key. The adjacent field displays "UNLOCK ALL PORTS Y/N".

3.   Enter **Y** to unlock all of the ports, or **N** to discontinue the port lock override. Responding with a **Y** unlocks all ports.

4.   Press the **Return** key.

7.8   ENABLING PORTS

The Port ENABLE Override function provides a fail-safe recovery when you cannot enable the chassis with remote inband SNMP.

To use the Port ENABLE Override:

1.   Use the arrow keys to highlight the **Port ENABLE Override** field.

2.   Press the **Return** key. The adjacent field displays "ENABLE ALL PORTS Y/N".

3.   Enter **Y** to enable all of the ports, or **N** to discontinue the port enable override. Responding with a **Y** enables all ports.

4.   Press the **Return** key.

CHAPTER 8

TRAP TABLE SCREEN

As an SNMP compliant device, the EMM-E6 can authenticate an SNMP request. The Trap Table defines the management stations to receive SNMP Traps for alarm/event notification.

8.1 ACCESSING THE TRAP TABLE SCREEN

To access the Trap Table Screen:

1. From the Features Selection Screen, use the arrow keys to highlight the **Component Trap Table** option.

2. Press the **Return** key. The Trap Table Screen, Figure 8-1, appears.

```
                    EMM-E6-960 LOCAL MANAGEMENT
                  Cabletron  EMM-E6 Revision 0.00.00
                            TRAP TABLE


       SNMP Community Name              Traps        Trap IP Address

       ctron                             N           132.177.118.24
       Mike                              Y           132.177.118.25
       Joe                               N           132.177.118.26
       Randy                             N           0.0.0.0
       Jerry                             N           0.0.0.0
       Chris                             N           0.0.0.0
       Scott                             N           0.0.0.0
       <CR>                              N           0.0.0.0




       SAVE      COMMUNITY NAMES   IP TABLE   SNMP TOOLS   CLI    RETURN
       F6              F7             F8           F9      F10
```

Figure 8-1. Trap Table Screen

8.2   TRAP TABLE SCREEN FIELDS

The Trap Table contains three modifiable fields. The fields, shown in Figure 8-1, allow the user to direct trap information to users on the network. The three fields are:

SNMP Community Name
Displays the community name associated with the network management station IP address to which the EMM-E6 sends trap messages.

Traps
Displays whether or not the EMM-E6 sends traps to the network management station with the associated IP address.

Trap IP Address
Indicates the IP address of the workstation to receive trap alarms from the EMM-E6.

8.3   CONFIGURING THE TRAP TABLE

1.   Using the arrow keys, highlight the **SNMP Community Name** field.

2.   Enter the community name that reflects the desired access level (e.g., the community name associated with the SUPER-USER access level) for SNMP trap information.
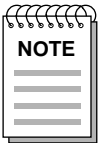
> **NOTE**
>
> *While any of the community names can be used by the Trap station, Network Management functions are best performed by a station with Super-user access to the EMM-E6.*

3.   Press the **Return** key.

4.   Using the arrow keys, highlight the **Traps** field and enter **Y** to send alarms from the EMM-E6 to that workstation, or **N** to prevent the EMM-E6 from sending alarms to that workstation.

5.   Press the **Return** key.

6.   Using the arrow keys, highlight the desired **Trap IP Address** field.

7.   Enter the IP address of the workstation to which you want the EMM-E6 to send traps. Use the XXX.XXX.XXX.XXX format with the value of XXX ranging from 0 to 254.

8.   Using the arrow keys, highlight the SAVE command.

9.   Press the **Return** key. The message "SAVED OK" appears.

> **NOTE**
>
> *If you exit without saving, you lose all edits.*
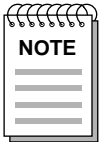
10. Exit the screen by either pressing the appropriate **Function key** to go directly to the desired LM screen, or by using the arrow keys to highlight the desired LM screen or the RETURN command, and then pressing the **Return** key. Using the RETURN command takes you back to the Feature Selection Screen.

The designated workstations, if properly configured and utilizing SNMP compliant remote management software, will now receive SNMP traps from the EMM-E6.

CHAPTER 9

SNMP TOOLS SCREEN

This section describes specific commands and features within the SNMP Tools screen. This screen allows you to access management information bases (MIBs), and varies according to your level of security access.

The following descriptions outline the super-user management capabilities. From SNMP Tools you can:

- review specifics about object identifiers (OIDs)
- edit configurable OIDs
- view OIDs sequentially from the originally requested OID.

9.1 ACCESSING THE SNMP TOOLS SCREEN

To access the SNMP Tools Screen:

1. From the Features Selection Screen, use the arrow keys to highlight the **SNMP Tool Support** option.

2. Press the **Return** key. The SNMP Tools Screen, Figure 9-1, appears.

```
                    EMM-E6-960 LOCAL MANAGEMENT
                    Cabletron EMM-E6 Revision 0.00.00
                              SNMP TOOLS

                       COMMUNITY NAME:  public
                         OID PREPEND:  1.3.6.1


  GET    SET   GETNEXT   WALK   RECALL-OID   STEP   CYCLES   REPEAT
  F6     F7      F8                  F9








                              RETURN
                                F10
```
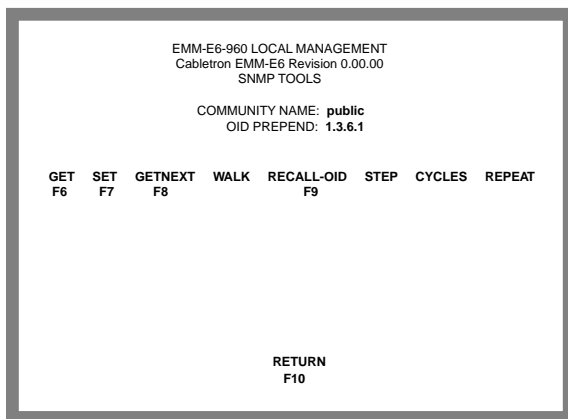
Figure 9-1. SNMP Tools Screen

9.2   SNMP TOOLS SCREEN FIELDS

The following describes the SNMP Tools Screen fields and commands.

COMMUNITY NAME
Identifies the community name MIB access level password.

OID PREPEND
Specifies the number prefix common to all object identifiers (OIDs) found in a MIB. The prefix '1.3.6.1' is the default. You can modify this field to suit your needs.

GET
Allows you to retrieve MIB objects, one at a time, using SNMP protocol.

SET
Lets you edit modifiable MIB objects, using SNMP protocol.

GETNEXT
Displays the next OID in the MIB tree by getting the next SNMP OID from a remote agent.

WALK
Scrolls through the MIB, leaf by leaf, from a user-specified object identifier. Leaves are objects, or instances of objects. After initializing a walk you see the following categories for each entry:

- Specified OID — identifies the number tag for that OID.
- Size — gives the number of bytes required to store the object.
- Data Type — gives the object's variable type (e.g., int=integer).
- Data Value — displays what the object identifier represents.

RECALL-OID
Recalls from memory the last OID used since powering up the board or re-entering the SNMP Tools screen.

STEP
Displays the MIB, step by step, with specific OID details.

CYCLES
Allows you to specify the number of **GET NEXT** requests to walk through and how much time elapses between each request.

REPEAT
Repeats the Get command, allowing you to monitor any changes to a specific OID.

9.3   THE SECURITY ACCESS LEVEL

Each MIB component that the EMM-E6 supports (e.g., RMON, DLM, Repeater Rev. 4, etc.) has its own "password" for each possible level of access (ranging from Basic Read-Only to Super-User).

Most MIB component community names default to "public." However, some components have specific community names (e.g., depending on what devices reside in the EMM-E6 managed hub, Repeater Rev. 4 uses separate community names for each channel in use – "channelA," "channelB," and/or "channelC").

NOTE
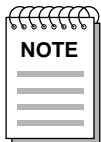
A complete list of Super-User community names (also called community strings) resides in the Cabletron proprietary chassis MIB. The MIB group chCompName provides the names of the MIB components. The MIB group chCompSUCommStr provides individual MIB component community names/strings.

The component information corresponds numerically – by last digit. In other words, each instance (i.e., OID element) in the chCompName group indicates its match in the chCompSUCommStr group.

In order to access a specific MIB's components, you must set the appropriate MIB password in the COMMUNITY NAME field.
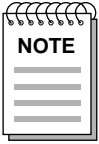
> **NOTE**
>
> *The default super-user password (public) allows you to access most MIB components. To change the SNMP Tools screen COMMUNITY NAME field, you must have super-user access to Local Management.*

To set the SNMP Tools screen COMMUNITY NAME:

1. Use the arrow keys to highlight the field to the right of **COMMUNITY NAME**.

2. Enter the community name necessary for super-user access for any specific MIB (e.g., channelA for Repeater Rev. 4 MIB).

3. Press the **Return** key. The community name changes.

9.4   GETTING AND SETTING OIDS

To get an OID:

1. Highlight **GET**, using the arrow keys.

2. Press the **Return** key. "<GET> OID (=|F9)" appears.

3. Enter an OID either by:

   • using the keyboard to enter the OID.

   > **TIP**
   >
   > *Save yourself some keystrokes by typing the OID minus the OID's prepend (i.e., given an OID prepend of 1.3.6.1, you enter 2.1.1.4.0, and the LM gets the MIB II sysContact OID 1.3.6.1.2.1.1.4.0).*

   • pressing **F9** to recall an OID already entered, and using the keyboard to modify the recalled OID as necessary.

4. Press the **Return** key. If there is no instance of that OID, the EMM-E6 displays "MIB_NO_INSTANCE." Otherwise, the EMM-E6 displays that OID's data type, length, and value.

To get the next OID:

1. Highlight **GETNEXT**, using the arrow keys.

2. Press the **Return** key. "<GETNEXT> OID (=|F9)" appears.

3. Enter the **OID**.

4. Press the **Return** key. If that OID does not exist, the EMM-E6 displays "MIB_NO_INSTANCE". Otherwise the EMM-E6 displays that OID's data type, length, and value.

> **TIP**
>
> *If you have previously entered an OID, press **F9** to recall that entry. You can use the arrow keys to modify the recalled OID, or if you have not previously entered the OID, type the OID minus the OID's prepend.*

To set an OID:

1. Highlight **SET**, using the arrow keys.

2. Press the **Return** key. "<SET> OID (=|F9)" appears.

3. Enter an **OID**.

4. Press the **Return** key. If that OID does not exist, the EMM-E6 displays "MIB_NO_INSTANCE". Otherwise the EMM-E6 displays:

{INteger String Null OId IP address Counter Gauge Timeticks OPaque} "DATA TYPE (name):"

> *If you have previously entered an OID, press **F9** to recall that entry. You can use the arrow keys to modify the recalled OID, or if you have not previously entered the OID, save yourself some keystrokes by typing the OID minus the OID's prepend.*

TIP

5. Enter the OID's **Data Type**.

NOTE
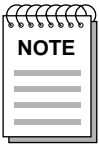
> *When setting a String, SNMP tools requests the kind of data you plan to enter — HEX or ASCII.*

6. Press the **Return** key. The EMM-E6 displays "SNMP OID DATA."

7. Enter the **Data**, or value of the OID.

8. Press the **Return** key. If the EMM-E6 accepts the entry, it displays "<SET> OPERATION CODE: XXXX <OK>"; otherwise, an error message appears.

9.5   SCROLLING THROUGH MIB OIDS

Viewing several object identifiers at one time allows you to quickly scan a MIB for the information that you need. The SNMP Tools screen provides several scroll options:

- Walk — scrolls through OIDs sequentially, from the initial OID.
- Cycle — allows you to specify how many GetNext commands to cycle through for one OID.
- Step — pages through the MIB, one OID at a time.

To walk through the MIB:

1. Highlight **WALK**, using the arrow keys.

2. Press the **Return** key. "<INITIAL> OID (=|F9)" appears.

3. Enter the OID.

4. Press the **Return** key. LM begins walking through the sublayers of the MIB available from the specified OID. Each OID in the list displays the specified OID, its size, its data type, and the data value.

5. Press any key to stop the walk, or wait for "***MIB WALK COMPLETED***" to appear on the screen.

To cycle through:

1. Highlight **CYCLES**, using the arrow keys.

2. Press the **Return** key. "ENTER CYCLE COUNT:" appears.

3. Enter the number of OID cycles that you want to scroll through.

4. Press the **Return** key. "ENTER CYCLE DELAY:" appears.

5. Enter the delay that you want (in seconds) between get next requests.

6. Press the **Return** key. "<INITIAL> OID (=|F9)" appears.

7. Enter the OID.

8. Press the **Return** key.

To step through:

1. Highlight **GETNEXT**, using the arrow keys.

2. Press the **Return** key. "<GETNEXT> OID (=|F9)" appears.

3. Enter the OID (only the suffix is necessary).

4. Press the **Return** key. The initial OID details, including its size, data type, and data value, appear.

5. Highlight **STEP**, using the arrow keys.

6. Press the **Return** key to page through the MIB to the next OID.

CHAPTER 10

ROUTER SETUP SCREEN

This chapter shows the Router Setup Screen, Figure 10-1, below. Using this screen the user can select the protocol to be used by any Routing Services previously installed in the EMM-E6. The user should use the Routing Services Manual to make the correct selections from the Router Setup Screen. The EMM-E6 User's Guide does not cover routing and all data on this window will be found in the Routing Services Manuals.

```
        EMM-E6-960 LOCAL MANAGEMENT
        Cabletron EMM-E6 Revision 0.00.00
                  SNMP TOOLS

        INTEGRATED ROUTER X.XX.XX

                ROUTER SETUP

            IP

            IPX

            DECnet




        INITIALIZE          RETURN
```
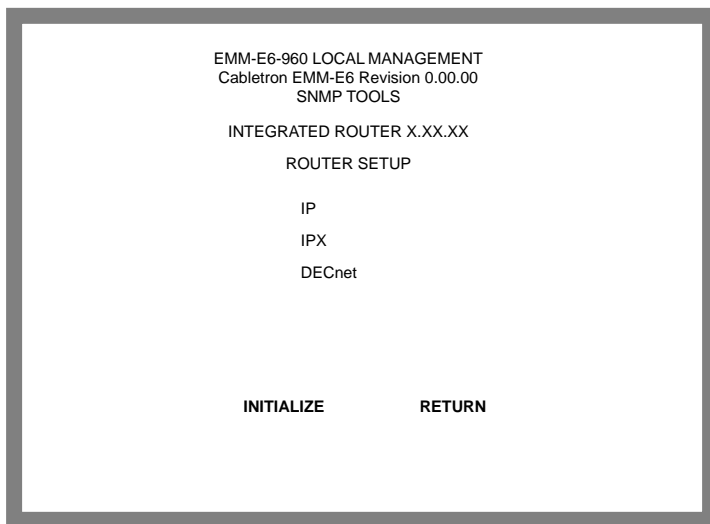
Figure 10-1. Router Setup Screen
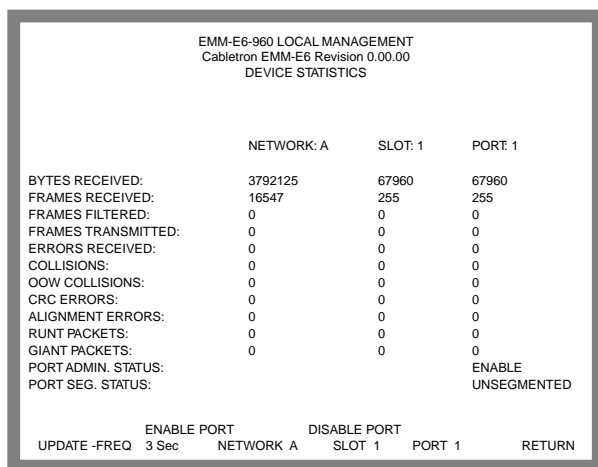
CHAPTER 11

DEVICE STATISTICS SCREEN

This chapter describes the features of the Device Statistics screen. Using this screen, you can view error, collision, and traffic statistics for the entire network, a selected slot, or a selected port. This screen also provides the option of enabling and disabling ports.

To access the Statistics screen:

1. From the Features Selection screen, use the arrow keys to highlight the **Device Statistics** option.

2. Press the **Return** key. The Device Statistics screen, Figure 11-1, appears.

```
                        EMM-E6-960 LOCAL MANAGEMENT
                        Cabletron EMM-E6 Revision 0.00.00
                              DEVICE STATISTICS


                              NETWORK: A        SLOT: 1          PORT: 1

BYTES RECEIVED:               3792125           67960            67960
FRAMES RECEIVED:              16547             255              255
FRAMES FILTERED:              0                 0                0
FRAMES TRANSMITTED:           0                 0                0
ERRORS RECEIVED:              0                 0                0
COLLISIONS:                   0                 0                0
OOW COLLISIONS:               0                 0                0
CRC ERRORS:                   0                 0                0
ALIGNMENT ERRORS:             0                 0                0
RUNT PACKETS:                 0                 0                0
GIANT PACKETS:                0                 0                0
PORT ADMIN. STATUS:                                              ENABLE
PORT SEG. STATUS:                                                UNSEGMENTED


              ENABLE PORT        DISABLE PORT
   UPDATE -FREQ  3 Sec    NETWORK  A    SLOT  1     PORT  1        RETURN
```

Figure 11-1. Device Statistics Screen

11.1   DEVICE STATISTICS

This section describes Device Statistics screen data fields.

BYTES RECEIVED
Displays the number of bytes received.

FRAMES RECEIVED
Displays the number of frames received.

FRAMES FILTERED
Displays the total number of frames filtered.

FRAMES TRANSMITTED
Displays the total number of frames transmitted.

ERRORS RECEIVED
Displays the total number of errors received.

COLLISIONS
Displays the number of collisions received.

OOW COLLISIONS
Displays the number of Out Of Window collisions. OOW collisions are usually caused by: The network being so long that the round trip propagation delay is greater than 51.2 µs (the collision domain is too large); a station somewhere on the network violating Carrier Sense and transmitting at will; or a cable somewhere on the network failing during the transmission of a packet.

CRC ERRORS
Displays the number of packets with bad Cyclic Redundancy Checks (CRC) that have been received from the network. The CRC is a 4 byte field in the data packet that ensures that the transmitted data that is received is the same as the data that was originally sent.

ALIGNMENT ERRORS
Displays the number of errors due to misaligned packets. Misaligned packets contain a non-integral number of bytes (i.e., some bytes contain fewer than 8 bits).

RUNT PACKETS

Displays the number of runt packets received from the network. A runt packet is less than the minimum Ethernet frame size of 64 bytes, not including preamble.

GIANT PACKETS

Displays the number of giant packets receivedfrom the network. A giant packet is greater than the maximum Ethernet frame size of 1518 bytes, not including preamble.

PORT ADMIN. STATUS

Displays the administrative status of the port selected. The two possible status messages are Enable or Disable.

PORT SEG. STATUS

Displays the segmentation status of the port selected. The two possible status messages are Segmented or Unsegmented. The EMM-E6 automatically partitions problem ports or interfaces (those having 32 consecutive collisions, and re-connects non-problem segments to the network.

11.2 DEVICE STATISTICS SCREEN COMMANDS

The Device Statistics screen provides several commands that allow you to access and manipulate various boards and ports. This section first gives a brief description of each command, and then explains how to use them.

ENABLE PORT

This command lets you enable the selected port.

DISABLE PORT

This command lets you Disable the selected port.

UPDATE-FREQ

This command lets you select the time interval between Network/ Slot/Port counter updates. You can choose update intervals in increments of 3 seconds, with the maximum interval being 99 seconds.

NETWORK
This command lets you select the network you want to monitor. The choices range from A to F, depending on the configuration of your network and the options available from this configuration. For example, if you do not have a Media Interface Module running on the A Channel, the EMM-E6 automatically disallows Channel A as a network selection.

SLOT
This command lets you select the MMAC hub slot that you want to monitor. The choices vary depending on the MMAC chassis you use. The far right slot is always slot number one (1).

PORT
This command lets you select and view port statistics for ports 1 through 26 of the device residing in the selected Slot.

11.2.1   Selecting an Update Frequency

The EMM-E6 updates the Device Statistics screen every three seconds by default. The EMM-E6 allows you to adjust this frequency in intervals of three seconds (maximum frequency is 99 seconds).

To adjust the UPDATE-FREQ:

1. Use the arrow keys to highlight the **UPDATE-FREQ** command.

2. Press the **Shift** and + keys together, or just the **-** key until the desired time/frequency appears (this number increments/decrements in 3 second intervals; minimum = 3 seconds; maximum = 99 seconds).

3. Press the **Return** key to set and save the changes to the UPDATE-FREQ field.

11.2.2   Selecting a Network/Slot/Port

When the Device Statistics screen first appears, statistics are displayed for Network 1, Slot 1, and Port 1. To view statistics for another Network, Slot, and Port, use the NETWORK X, SLOT X, or PORT X commands at the bottom of the screen.

To select a Network, Slot, or Port:

1.   Using the arrow keys, highlight the NETWORK X, SLOT X, or PORT X command.

2.   Press the **Shift** and + keys together, or just the **-** key until the desired network, slot, or port number appears.

3.   Press the **Return** key. Statistics associated with the selected network, slot, or port appear.

11.2.3   Enabling Ports

The ENABLE PORT command lets you enable the port selected in the PORT command. You must first use the PORT command to select the desired port.

To set the PORT ENABLE command:

1.   Use the arrow keys to highlight the ENABLE PORT command at the bottom of the screen.

2.   Press the **Return** key. The PORT ADMIN. STATUS field displays "ENABLE".

11.2.4   Disabling Ports

The DISABLE PORT command lets you disable the port selected in the PORT command. You must first use the PORT command to select the desired port.

To set the PORT DISABLE command:

1. Use the arrow keys to highlight the DISABLE PORT command at the bottom of the screen.

2. Press the **Return** key. The PORT ADMIN. STATUS field displays "DISABLED".

11.3   EXITING THE DEVICE STATISTICS SCREEN

To exit the Device Statistics screen:

1. Use the arrow keys to highlight the RETURN command at the bottom of the screen.

2. Press the **Return** key. The Feature Selection screen appears.

CHAPTER 12

COMMAND LINE INTERFACE SCREEN

The Command Line Interface (CLI) Screen, Figure 12-1, will function in future releases of the EMM-E6.

```
                    EMM-E6-960  LOCAL MANAGEMENT
                    Cabletron EMM-E6 Revision 0.00.00
                           CLI INFORMATION




                    ┌─────────────────────────────────────┐
                    │    THIS SCREEN RESERVED FOR THE      │
                    │ CABLETRON COMMAND LINE INTERFACE     │
                    └─────────────────────────────────────┘






 COMMUNITY NAMES     IP TABLE      TRAP TABLE  SNMP TOOLS     RETURN
       F7               F8             F9         F10
```
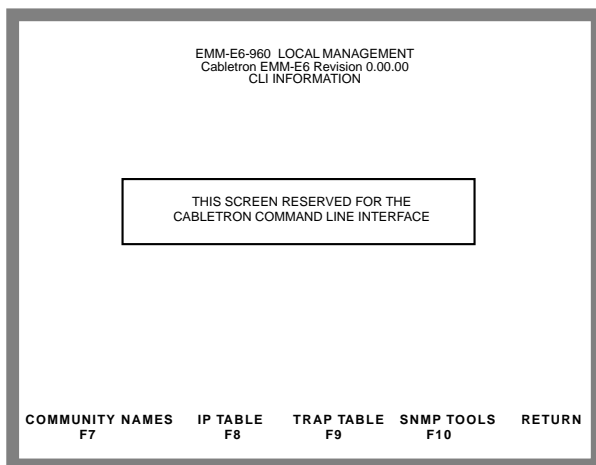
Figure 12-1. EMM-E6 CLI Information Screen

CHAPTER 13

MIB NAVIGATOR

This chapter describes the procedures required to access the MIB Navigator residing on the EMM-E6. The MIB Navigator Command Set is described and examples of each command are provided.

13.1 MANAGING DEVICE MIBs

The MIB Navigator allows access to a command set from which you can configure and manage your device. The MIB Navigator enables you to manage objects in the device MIBs (Management Information Bases). MIBs are databases of objects used for managing the device and determining your EMME's configuration. The commands within the MIB Navigator allow you to view and modify a device's objects.

The MIB Navigator views the MIB tree hierarchy as a directory (Figure 13-1). Each layer is numerically encoded, so that every branch group and leaf object in the MIB is identified by a corresponding number, known as an Object Identifier (OID). This allows the MIB Navigator to navigate through the MIB and access the manageable leaf objects.
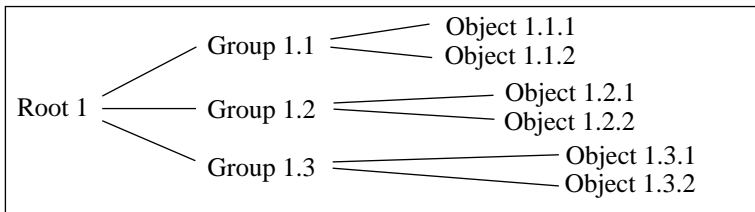
Figure 13-1. Hierarchical MIB Tree Structure

Often an ASCII name is assigned to a leaf object's OID, making it more readable. To identify the value for the object "ip Forwarding" you would use the OID (/1/3/6/1/2/1/4/1), or its ASCII name (/iso/org/dod/internet/ mgmt/mib-2/ip/ipForwarding).

13.2 ACCESSING THE MIB NAVIGATOR

The MIB Navigator function resides on your Cabletron device (EMM-E6, ETWMIM, ESXMIM, etc.). Access the MIB Navigator in-band, through a device (i.e., workstation) connected to the same network or internetwork, using a Telnet connection.

To access the MIB Navigator, perform the following actions from a PC or workstation:

1. Telnet to a device by typing **telnet** followed by pressing the **Return** key.

    The *telnet >* prompt will appear.

2. At the *telnet >* prompt enter **open** and the IP address of the device followed by pressing the **Return** key, i.e.,

    telnet> open 123.231.213.132

3. The following messages will appear:

    .Trying 123.231.213.132

    Connected to 123.231.213.132

    Password:

4. Enter your password at the **Password***:* prompt and press the **Return** key. For security reasons, the password does not display when typed.
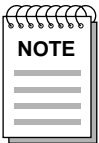
> **NOTE**
>
> *The password that you use is specific to the MIB that you are accessing.*

5. The MIB Navigator prompt, MIBNav ->, appears and you have access to the MIB Navigator commands.

13.3   MIB NAVIGATOR COMMAND SET OVERVIEW

There are three categories of commands in the command set.

- **Navigation Commands** - Allows the user to access and manage the MIB for the device running the MIB Navigator. Some of commands also provide user community-string information. The commands are as follows:

    - branch   - cd   - ctron   - dir
    - get   - ls   - mib2   - next
    - pwd   - set   - show   - su
    - tree   - whoami

- **Built-In Commands** - Allows the user to access and manage network devices connected to the device running the MIB Navigator. The commands are as follows:

    - arp   - defroute   - netstat   - ping
    - snmpbranch - snmpget   - snmpset   - snmptree
    - traceroute

- **Special Commands** - Allows the user to exit from the MIB Navigator. The commands are as follows:

    - done   - quit   - exit

13.3.1   Conventions For MIB Navigator Commands

The following conventions are used for denoting commands:

- Information keyed by the user is shown in this helvetica font.

- Command arguments are indicated by two types of brackets:

    - required arguments are enclosed by [].
    - optional arguments are enclosed by <>.

MIB Navigator command conventions are as follows:

- To abort the output or interrupt a process the escape character is ^C (where ^ equals the Control key).

- A slash (/) proceeding an OID issues that command from the root directory regardless of where you are in the MIB. If no slash precedes the OID the command issues from your current MIB location.

- Dot notation (1.1.1.1) is equivalent to slash notation (1/1/1/1). Use slash notation with the navigational commands, and the dot notation with the built-in commands that are using SNMP to access and manage network devices.

13.3.2   Navigation Commands

The following provides a brief description, the proper format, and an example of each Navigation command.

branch	The branch command displays all of the leaves in the MIB tree below a specified path. The information displayed includes the path name, the object ASCII name, the type of object (i.e., integer, counter, time tick, etc.), and the current value. Format:branch [PATH]
	Example MIBNav> branch /1/3/6/1/2/17

Navigation Commands (cont'd)

cd | Use this command to change directories within a MIB subtree. The path specified must be valid.
This command has two special subtree options:

..   - Moves you to one subtree above the current one.

/   - Moves you to the root.

Format: cd [PATH]

Example   MIBNav> cd iso/org/dod/internet/mgmt

ctron | The ctron command enables you to change directories directly to the Cabletron MIB (1.3.6.1.4.1.52) without keying in the entire path.

Format: ctron

Example   MIBNav> ctron

Navigation Commands (cont'd)

dir, ls	Each of these commands displays the contents of a specified sub-tree (the current directory displays if you do not specify a sub-tree).

Options can be used separately or combined. When no option is used the ASCII name of the leaf object displays. The three options available with these commands are:

   -l   Displays all instances of the object's OID value (/1/3/6/) and ASCII leaf object name (internet).
   -p   Displays all entries from the current directory including the object's path name.
   -d   Displays only directory entries in the tree.

Format: dir (ls)
               dir -l
               dir -lpd |

Example	MIBNav> dir

Example	MIBNav> dir -l
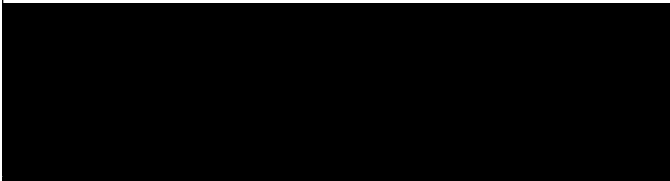
get	The get command provides you with the value of a specific managed object. The command is valid only for leaf entries in the current MIB tree, or for managed objects in the MIB.

Format: get <OBJECTID> |

Example	MIBNav> get /1/3/6/1/2/1/1/1

Navigation Commands (cont'd)

help The help command provides a list of available MIB Navigator commands. The command also provides help for individual MIB Navigator commands.

   Format: help (general help)
               help <COMMAND> (specific help)

Example	MIBNav> help su

mib2 The mib2 command enables you to change directories directly to MIB II (1.3.6.1.2.1) without keying in the entire path.

   Format: mib2

Example	MIBNav> mib2

next The next command enables you to determine the next leaf in a specified path within the managed device's MIB. This command operates much like the SNMP GETNEXT operator.

   Format: next [PATH]

Example	MIBNav> next /1/3/6/1/2/1

Navigation Commands (cont'd)

pwd	The pwd command displays the full path name for the directory in which you are currently working. Format: pwd

	Example MIBNav> pwd

set	The set command enables you to set the value of a managed object. This command is valid only for leaf entries in the current MIB tree, or for managed objects in the MIB.
	
	If a leaf does not exist for the given path, you will be asked what value to assign it. The following lists possible value types:
	
	  (i)nteger - number
	  (c)ounter - number
	  (g)auge - number
	  (t)ime ticks - number
	  o(p)aque - "value" (with quotation marks)
	  (s)tring - "value" (with quotation marks)
	  (o)id - number/number.number
	  (a)ddress - IP address/dotted decimal
	  (m)ac - physical address/hex string
	  (n)ull - no type
	
	Format: set <OBJECTID> <VALUE>

	Example MIBNav> set /1/3/6/1/2/1/1/5 "1st Floor" Example MIBNav> set /1/3/6/14/1/52/1/6/4/7 122.1.1.1

Navigation Commands (cont'd)

su The su command enables you to change your community name to allow for different access to the MIB. The community name that you enter allows you either Basic Read, Read Only, Read/Write, or Super-User access to that device's MIBs, depending on the level of security access assigned the password through the Local Management Community Table. Refer to Chapter 6 on how to establish a community name password.

Format: su [COMMUNITYNAME]

Example   MIBNav> su public

tree The tree command provides a display of the entire MIB for the device. Leaves and associated values are displayed in columns.

Format: tree

Example   MIBNav> tree

Navigation Commands (cont'd)

whoami | The whoami command displays your community string and access privileges to the MIB. When using the whoami command one of these four access levels will display: Basic Read, Read Only, Read/Write, and Super User.

Format: whoami

Example	MIBNav> whoami
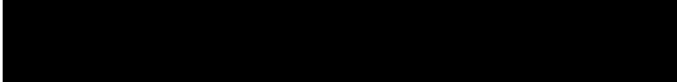
13.3.3   Built-In Commands

The following provides a brief description, the proper format, and an example of each Built-In command.

arp | 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. Superuser 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. The device's media connection occurs in one of the following ways:

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

Format   arp -a (to view cache data)

arp -d <INTERFACENUM> <IPADDRESS> (deletes an IP address entry)
arp -s <INTERFACENUM> <IPADDRESS> <MACADDR> (adds a static entry)

Example   MIBNav> arp -a

Example   MIBNav> arp -d 1 122.144.52.68

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

Built-In Commands (cont'd)

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

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

Format   netstat -i

                netstat -r

Example   MIBNav> netstat -i
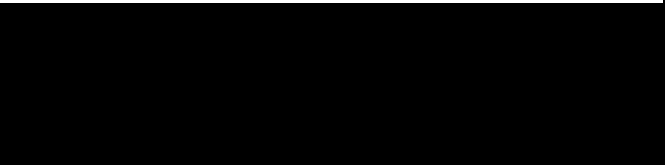
Example   MIBNav> netstat -r
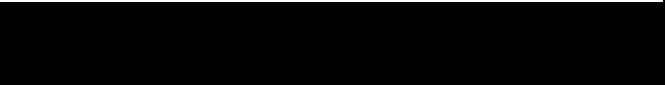
ping | The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Format: ping <IPADDRESS>

Example   MIBNav> ping 122.144.40.10

Built-In Commands (cont'd)

snmp-branch

The snmpbranch command enables you to query another SNMP device. The command provides a display of objects that match the specified OBJECT-ID. If no match is made, no object will display.

Format: snmpbranch <IPADDRESS>
            <COMMUNITY STRING> <OBJECT-ID>

Example   MIBNav> snmpbranch 2.4.8.1 public 1.3.6.2.1.1

snmpget

The snmpget command enables you to query another SNMP device to obtain a value for a specified object. This command requires the appropriate community string and object id.

Format: snmpget <IPADDRESS>
            <COMMUNITY-NAME> <OBJECT-ID>

Example   MIBNav>snmpget 22.44.61.22 public 1.3.6.1.2.1.1.1.0

Built-In Commands (cont'd)
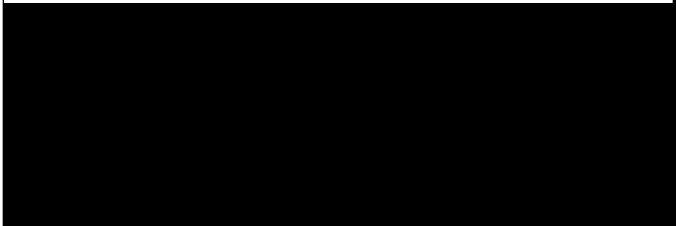
snmpset The snmpset command enables you to set the value of an object in other SNMP devices. This command requires the appropriate community string and OID.

When defining a new leaf, the set command prompts you for a value type. Possible value types are as follows:

(i)nteger - number
(c)ounter - number
(g)auge - number
(t)ime ticks - number
o(p)aque - "value" (value with quotation marks)
(s)tring - "value" (value with quotation marks)
(o)id - number/number.number
(a)ddress - IP address/dotted decimal
(m)ac - physical address/hex string
(n)ull - no type

Format: snmpset <IPADDRESS> <COMMUNITY-
                   NAME> <OBJECT-ID> <VALUE>

Example   MIBNav> snmpset 122.44.1.2 public

snmptree The snmptree command provides a display of all objects in the device and their corresponding values.

Format: snmptree <IPADDRESS>
                   <COMMUNITY-NAME>

Example   MIBNav> snmptree   122.144.89.10 public
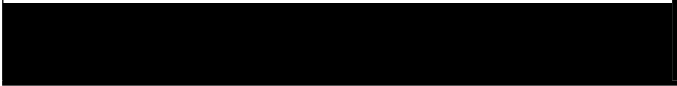
Built-In Commands (cont'd)

traceroute 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.

Format: traceroute <IPADDRESS>

Example   MIBNav> traceroute 122.144.11.52

13.3.4   Special Commands

The following provides a brief description, the proper format, and an example applicable to each Special command.

done, quit, exit	These commands enable you to exit from the MIB Navigator and return to the operating system. Format: done
	Example MIBNav> done

CHAPTER 14

TROUBLESHOOTING

This chapter includes information for troubleshooting network and EMM-E6 operational problems. The following sections describe the EMM-E6's LANVIEW LEDs, provide a troubleshooting checklist, and explain how and when to reset the EMM-E6.

14.1   USING LANVIEW

The EMM-E6 uses the Cabletron Systems built-in visual diagnostic and status monitoring system called LANVIEW. With LANVIEW, you can quickly scan the EMM-E6 LEDs to observe network status or diagnose network problems.
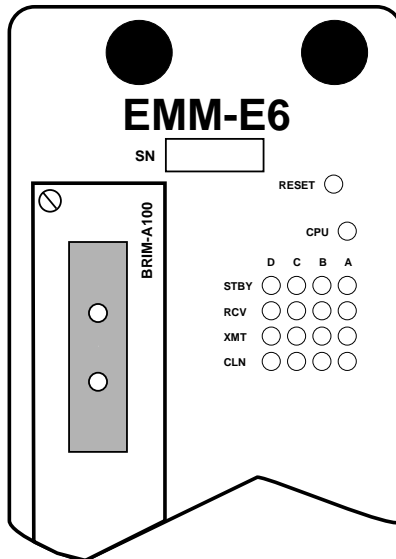
Figure 14-1. LANVIEW LEDs

Table 14-1. LANVIEW LEDs

LED	Color	Description	Error Condition/ Recommended Action
CPU	Multicolor Green Red	Flashing Green indicates that the board is operating properly.	If OFF, or Red, the board has a problem. Press the reset switch on the EMM-E6 front panel to re-initialize the board. If the board does not re-initialize, it has probably failed. Call Cabletron Technical Support.
STBY A,B,C,D (Standby)	Yellow	Indicates packets will not be forwarded as the Spanning Tree Algorithm has put the corresponding Bridge Port into a standby mode due to detecting a data loop condition.	Network Management has placed the EMM-E6 in a Standby condition; a data loop condition exists. Check with your Network Administrator to find out if the EMM-E6 was placed in Standby on purpose. If a Data loop does exist, reconfigure the network to remove the data loop.
RCV A,B,C,D (Receive)	Yellow	LED flashes to indicate that a segment is receiving a frame.	If none of the receive LEDs is flashing, the EMM-E6 is not receiving frames on any of the segments. Check that each module is firmly installed in the MMAC. Ensure that all connected ports are enabled.

Table 14-1. LANVIEW LEDs (Continued)

LED	Color	Description	Error Condition/ Recommended Action
XMT A,B,C,D (Transmit)	Green	LED flashes to indicate that a segment is transmitting a frame. If not connected to the LAN, the LED flashes every two seconds to indicate it is transmitting BPDU frames.	If none of the transmit LEDs is flashing, the EMM-E6 is not transmitting frames on any of the segments. Contact Cabletron Technical Support for assistance.
CLN (Collision)	Red	Collision detected on a segment. When the LAN is operating properly, occasional flashing is normal.	Excessive flashing, or a solid light, indicates an inordinate number of collisions. Ensure that the SQE test is disabled for any transceiver connected to the EMM-E6's external channels (D, E, or F). Check cabling for data loops or defective cables.

14.2   TROUBLESHOOTING CHECKLIST

If your EMM-E6 is not operating properly, the following checklist describes some of the problems that may occur with the EMM-E6 installed in an MMAC, possible causes for the problem, and suggestions for resolving the problem.

Table 14-2. Troubleshooting Checklist

Problem	Possible Causes	Recommended Action
No LEDs on.	Loss of Power to the MMAC. EMM-E6 not properly installed.	Check the proper installation of the MMAC power supply module and its access to a live outlet. Check that the MMAC has adequate power. Some configurations, especially those including FDDI modules, require that more than one power supply be installed in the MMAC. Check to see that the power supply LEDs are green. Reset EMM-E6 by removing it from chassis and reinserting according to directions in Chapter 3. Ensure that all fasteners are tightened.
No Local Management Password screen.	Terminal setup is not correct. Improper console cable/UPS cable pinouts.	Refer to Chapter 4 for proper setup procedures. Refer to Appendix A for proper console/ UPS port pinouts.
Cannot contact the EMM-E6 from in-band management.	Improper Community Names Table. EMM-E6 does not have an IP address. No link to device. Packets are being bridged by a permanent entry.	Refer to Chapter 6 for Community Names Table setup and Chapter 7 for IP address assignment procedures. Check link to device. Check Static Database.

Table 14-2. Troubleshooting Checklist (Continued)

Problem	Possible Causes	Recommended Action
A port on a MIM managed by the EMM-E6 cannot access the network, while other ports on the same MIM are able to access.	The port is either off or segmented. Port cable is defective.	Enable the port via local or remote management. Try connecting the port with a different cable.
User parameters (IP address, Device and Module name, etc.) are lost when device is powered down.	Switch 7 has been toggled and user-entered parameters have been reset to factory default. NVRAM may be defective.	See Chapter 3 for information on the NVRAM switch setting. If NVRAM is defective, call Cabletron Technical Support.
No power to an external transceiver connected to an EPIM-A.	EPIM is defective. AUI cable is defective.	Replace EPIM. Replace AUI cable.
High number of collisions on EPIM port.	External transceiver has SQE enabled.	Disable SQE.
Port(s) go into standby for no apparent reason.	Configurations where devices connected across EMM-E6 channels can cause the EMM-E6 to detect a looped condition.	Discuss these configurations with Cabletron Technical Support before implementing them into your network.

14.3   USING THE RESET SWITCH

The EMM-E6 incorporates a recessed reset switch, located above the LEDs (see Figure 14-1). This reset switch initializes the EMM-E6 processor. This switch does NOT initialize Non-Volatile Random Access Memory (NVRAM), the non-volatile random access memory where the EMM-E6 stores network management parameters.

To use the reset switch, use a pen or pencil to press the switch in. When this is done, the EMM-E6 initializes itself.

CHAPTER 15

IMAGE FILE DOWNLOAD

This chapter provides instructions for downloading an image file to the EMM-E6 using three different methods; altering hardware switch settings to force the module to accept new firmware, through UNIX operating System commands, and by setting specific MIB OID strings. To set OID strings, you can use the SNMP Tools screen described in Chapter 9 of this User's Guide or any MIB walking tool. Refer to specific MIB walking tool documentation for instructions on how to set MIB OID strings.
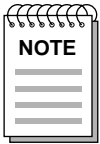
> **NOTE**
>
> *You can also download an image file using various remote management packages such as Cabletron's Remote LANVIEW/Windows, SPECTRUM, SPECTRUM Element Manager, or the appropriate SPECTRUM Portable Management Application. Refer to specific package documentation for image file download procedures.*

The EMM-E6 supports the following Download applications:

- **Forced Download** - Forcing a download of firmware images is accomplished using Switch 6 of the EMM-E6 and a pre-configured reverse address resolution protocol server holding the firmware image.

- **Standard Local Download** - the EMM-E6 automatically disables management while you download the new firmware image. You can **not** perform a Standard Download from a BRIM port.

- **Remote Runtime Download** - the EMM-E6 continues to operate without interruption while you download the new firmware image. The EMM-E6 stores the new image in Flash memory. It continues to operate with the old firmware image executing in processor memory until you reset the EMM-E6. You can perform a Runtime Download from any network port, including the BRIM.

15.1 GETTING STARTED

Cabletron ships backup copies of image files for all of its intelligent devices. The first file, suffixed with **.hex** (after it has been decompressed from a **.zip**) is for Standard Local Downloading (any port, except the BRIM). The second file, suffixed with **.fls** (after it has been decompressed from a **.zip**) is for Remote Runtime Downloading through any network port, including the BRIM.

Before you can download the image to a device, you must:

- load the image file onto your network rarp server
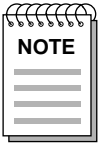
> **NOTE**
>
> *For information on setting up a workstation as a rarp server, refer to your specific workstation documentation. This documentation includes limited information and guidelines for setting up a UNIX workstation to act as a reverse address resolution protocol (rarp) server.*

- decompress the image file.
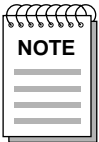
> **NOTE**
>
> *For your convenience, Cabletron includes the PKUNZIP utility for easy decompression of the "zipped" file. If you are using a UNIX workstation as a rarp server, and you do not have a decompression utility that recognizes the PKZIP format, you can obtain a copy of a UNIX decompression utility or the image file from the Cabletron Systems FTP server. Contact Cabletron Technical Support for details.*

15.2   FORCED DOWNLOAD WITH UNIX

Downloading an EMM-E6 image file with a UNIX workstation requires setting up a management station, and forcing the download. To force a download, you can use mode switch 6 on the EMM-E6 or set specific MIB OIDs.
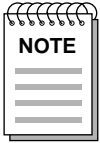
> **NOTE**
>
> *You can also download with other UNIX or DOS remote management packages. Refer to specific package documentation for image file download procedures.*

Due to variations between UNIX systems and individual configurations, this section provides only *GUIDELINES* for configuring a UNIX workstation to perform an image file download. The instructions include command examples, where appropriate. Bold lettering in examples indicates operator entry.
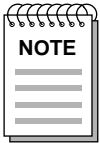
> **NOTE**
>
> *If unsure how to properly configure your UNIX workstation using these guidelines, contact your Systems Administrator.*

Before you start:

- Editing ethers or hosts files requires Root/Superuser access.

- Downloading an image file requires setting up your UNIX workstation as a reverse address resolution protocol (rarp) server.

To set up a UNIX workstation:

1. Edit the /etc/ethers file by adding the EMM-E6 MAC address, followed by a unique name (e.g., 00:00:1d:32:0c:1b EMME6).

2. Edit the /etc/hosts file by adding the EMM-E6 MAC address and follow it with the same unique name you used in step one above. (e.g., 00:00:1d:32:0c:1b EMME6).

3. If you already have a /tftpboot directory, confirm the rarp setup of your workstation as follows:

   Request a process status and grep for rarpd
   (e.g., unix% **ps -aux | grep rarpd**).

   The following information represents a typical output:

   ```
   user   161  7.7  1.2  32  184  p3  S   12:00  grep rarpd
   root    87  0.0  0.9  48  136  ?   S   11:05  rarpd -a
   root    88  0.0  0.0  24   0   ?   IW  11:05  rarpd -a
   ```

The term rarpd -a, located at the end of the root string, indicates rarp is active. If rarp is NOT running, only the grep process appears.

4. If you do NOT have a /tftpboot directory, then you must create one (e.g., unix% **mkdir tftpboot**), and start the rarp daemon (e.g., unix% **rarpd -a**).

5. Ensure that the /tftpboot directory is not owned (e.g., unix% **chown nobody tftpboot**).

6. Store the hex image file in the /tftpboot directory as emme6.hex.
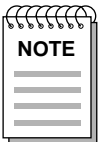
NOTE	*This step requires decompression of the zipped image file. If you do not have a UNIX unzip utility, access to a PC with pkunzip, or a way to FTP the decompressed image to your UNIX workstation, contact Cabletron Technical Support.*

7. Edit the /etc/inetd.conf file by removing anything prior to the tftpboot daemon (e.g., the # sign) that comments-out the line.

8. Kill the inetd process (e.g., unix% **kill -HUP 'process ID number'**), and then restart the process (e.g., unix% **inetd**), to enable the revised inetd.conf file.
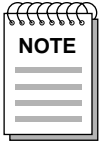
NOTE   *You must request a process status and grep for inetd to obtain the process ID number (see step 3 above).*

To force a download using the EMM-E6 download switch:

1. Remove the safety bars from the MMAC chassis.

2. Unscrew the knurled knobs at the top and bottom of the EMM-E6 front panel.

3. Slide the MIM out of the chassis until you can easily access the EMM-E6 switch panel located at the bottom of the board.

4. Change the state of EMM-E6 mode switch 6. For example, if the switch is in the "OFF" position, move it to the "ON" position and leave it there. This change in position activates the download process after you reinstall the board.
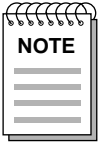
> **NOTE**
>
> *The EMM-E6 boot PROM must recognize the switch position change to initiate a download sequence. This means you must power-up the EMM-E6 at least one time for it to load initial switch positions into memory.*

5. Follow the installation procedures from Chapter 3 to re-install the EMM-E6 properly.

Image file download takes several minutes. While downloading, the EMM-E6 CPU LED flashes and the XMT/RCV pair receiving the image flickers rapidly.

The EMM-E6 Boot-up Diagnostics indicate a file transfer from a server is in progress. After the image file download is complete, verify that Local Management displays the correct image file (FW) version number.

15.3   STANDARD LOCAL DOWNLOAD

Table 15-1 provides a step by step procedure for downloading the firmware image file. This section provides specific MIB OIDs, their names, and the required setting for proper image file download. Refer to your specific MIB walking tool documentation for instructions on how to set MIB OID strings.

The Download OIDs for Cabletron products reside in Cabletron enterprise MIBs (group 52). The specific OIDs necessary to perform an image file download reside in the common download group under ctDL (Cabletron Download). The full OID string to reach this group is:

<p style="text-align:center">1.3.6.1.4.1.52.4.1.5.8.1</p>

When performing the steps in Table 15-1, keep the following in mind:

- You must follow the steps in order.
- Enter the IP address of the tftp server in standard dotted decimal notation (e.g., 132.177.118.24).
- Enter the FULL path to the image file in the ctDLTFTPRequest OID, including the name of the image file (e.g., c:\tftpboot\EMME6.hex).

<p style="text-align:center">Table 15-1. Standard Download Procedure</p>

Step	OID Name	OID Number	Data Type	SNMP OID Data
(1).	ctDLForceOnBoot	1.3.6.1.4.1.52.4.1.5.8.1.**1.0**	integer	1
(2).	ctDLCommitRAMToFlash	1.3.6.1.4.1.52.4.1.5.8.1.**2.0**	integer	1
(3).	ctDLTFTPRequestHost	1.3.6.1.4.1.52.4.1.5.8.1.**4.0**	IP address	Enter the IP address of the tftp server.
(4).	ctDLTFTPRequest	1.3.6.1.4.1.52.4.1.5.8.1.**5.0**	string (ASCII)	Enter the path to the image file.
(5).	ctDLInitiateColdBoot	1.3.6.1.4.1.52.4.1.5.8.1.**3.0**	integer	1

15.4 REMOTE RUNTIME DOWNLOAD
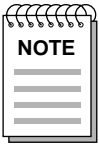
> **NOTE**
>
> *If the Runtime Download is interrupted, the Firmware Image in Flash memory will be erased. The EMM-E6 will continue to operate until it is either Reset or Powered OFF and ON. After either of these events, the EMM-E6 can download a Firmware Image from a BootP server ONLY! The process of configuring a BootP Server is discussed at length in Cabletron's "Installing and Using Remote LANVIEW for Windows". Although Runtime Download is a powerful network operations & firmware management feature, careful consideration should be given to both the timing (best when network usage is lowest) and network stability (especially downloads over a WAN link) at the time of the planned download.*

Table 15-2 provides a step by step procedure for downloading the firmware image file. This section provides specific MIB OIDs, their names, and the required setting for proper image file download. Refer to your specific MIB walking tool documentation for instructions on how to set MIB OID strings.

The Download OIDs for Cabletron products reside in Cabletron enterprise MIBs (group 52). The specific OIDs necessary to perform an image file download reside in the common download group under ctDL (Cabletron Download). The full OID string to reach this group is:

1.3.6.1.4.1.52.4.1.5.8.1

When performing the steps in Table 15-2 keep the following in mind:

- You must follow the steps in order.
- Enter the IP address of the tftp server in standard dotted decimal notation (e.g., 132.177.118.24).
- Enter the FULL path to the image file in the ctDLTFTPRequest OID, including the name of the image file (e.g., c:\tftpboot\EMME6.fls).

Table 15-2. Runtime Download Procedure

Step	OID Name	OID Number	Data Type	SNMP OID Data
(1).	ctDLTFTPRequestHost	1.3.6.1.4.1.52.4.1.5.8.1.**18.0**	IP address	Enter the IP address of the tftp server.
(2).	ctDLTFTPRequest	1.3.6.1.4.1.52.4.1.5.8.1.**19.0**	string (ASCII)	Enter the path to the image file.
(3).	ctDLOnLineDownload	1.3.6.1.4.1.52.4.1.5.8.1.**16.0**	integer	**1** = Default setting (normal operation). **2** = **forceDownLoad**. The new image downloads to Flash memory. The EMM-E6 does not use the new image until you press the Reset button. **3** = **forceDownLoad-Reset**. The new image downloads to Flash memory. The EMM-E6 automatically resets upon completion of the download.
(4)	ctDLOperStatus (This OID monitors the progress of the Runtime Download.)	1.3.6.4.1.52.4.1.5.8.1.**17.0**	Integer	**2** = Indicates that a TFTP download request has been received but has not yet been activated. **3** = Indicates normal operation. The download started and finished normally and no reset was specified or a download has not been started. **4** = Indicates that a download is in progress. **5** = Indicates that a download was started but has terminated due to an error.

Table 15-2. Runtime Download Procedure (Continued)

Step	OID Name	OID Number	Data Type	SNMP OID Data
NOTE: If you selected **forceDownLoadReset** at Step 3, then DO NOT CONTINUE, you have completed all necessary settings. **NOTE**: If you selected **forceDownLoad** at Step 3, then you can reset the EMM-E6 at a later time. You can reset the EMM-E6 remotely using the ctDLInitiateColdBoot OID described at Step 5 or manually using the Reset Button or Cycle Power.				
(5).	ctDLInitiateColdBoot	1.3.6.1.4.1.52.4.1.5.8.1.**3.0**	integer	1

APPENDIX A

EMM-E6 SPECIFICATIONS

This appendix provides the operating specifications for the Cabletron Systems EMM-E6. Cabletron Systems reserves the right to change these specifications at any time without notice.

A.1 BRIDGING FUNCTIONALITY

FLASH Memory: 2 MB (expandable to 14 MB)

Shared Sonic Memory: 4 MB (expandable to 12 MB)

Internal Processor: Intel 80960

Read Only Memory: 128K

Non-Volatile RAM: 128K

Ethernet Controller: 4 DP83932 Controllers

CPU Memory: 8 MB (expandable to 12MB)

Packet Filter Rate
(max. viewed per second):   30,000 packets

Packet Forward Rate
(max. forwarded per second):   22,000 packets

Forwarding Latency: 91 µs min.

Ageing Time: 5 minutes (default)

Filtering Database: 8,191 max.

A.2 REPEATER FUNCTIONALITY

Delay Times
(port x in to port x out)

Start of Packet:	1,450 ns max.
Collision to JAM:	1,550 ns max.

Preamble

Input:	Minimum of 40 bits to a max. of 64 bits required.
Output:	64 bits min. (last 2 bits = 1,1).

JAM Output:	If a collision occurs on one of the segments, a pattern of 1,0 is sent to the other segments.
Minimum Packet Repeated:	96 bits including preamble. (Packet fragments are extended using the JAM [1,0] data pattern.)
FAULT Protection:	Each segment will disconnect itself from the other segments if 32 consecutive collisions occur, or the collision detector of a segment is on for longer than approximately 2.4 ms. This FAULT protection will reset automatically after one packet is transmitted onto the FAULT protected segment without causing a collision.

A.3   COM 1 PORT

Type: Standard RJ45 port

Pin 1	Transmit Data (XMT)	From COM 1 port
2	Data Set Ready (DSR)	To COM 1 port
3	Not used	
4	Receive Data (RCV)	To COM 1 port
5	Signal Ground (GND)	
6	Data Terminal Ready (DTR)	From COM 1 port
7	Not used	
8	Not used	

A.4   COM 2 PORT

Type: Standard RJ45 port

Pin 1	Transmit Data (XMT)	From COM 2 port
2	Data Set Ready (DSR)	To COM 2 port
3	Not used	
4	Receive Data (RCV)	To COM 2 port
5	Signal Ground (GND)	
6	Data Terminal Ready (DTR)	From COM 2 port
7	Not used	
8	Not used	

A.5   ENVIRONMENTAL REQUIREMENTS

Operating Temperature: +5° to +40°C (+41° to +104°F)

Non-operating Temperature: -30° to +90°C (-22° to +194°F)

Operating Humidity: 5 to 95% (non-condensing)

A.6   SAFETY

This unit meets the safety requirements of UL 1950 (without D3 deviations), CSA C22.2 No. 950, and EN 60950; the EMI requirements of FCC Part 15 Class A, EN 55022 Class A, and VCCI Class I; and the EMC requirements of EN 50082-1, including IEC 801-2 (ESD) levels 1 through 4, IEC 801-3 (Radiated Susceptibility) levels 1 through 4, and IEC 801-4 (EFT/B) levels 1 through 4.

WARNING   *It is the responsibility of the person who sells the system of which the EMM-E6 will be a part to ensure that the total system meets allowed limits of conducted and radiated emissions.*

A.7   PHYSICAL PROPERTIES

Dimensions: 34.04D x 29.21H x 7.64W cm.
                            (13.4D x 11.5H x 3.0W in.)

Weight

  Unit: 1.25 kg (2.75 lbs.)
  Shipping: 1.74 kg (3.83 lbs.)

A.8 EPIM-T (10BASE-T TWISTED PAIR PORT)

Internal Transceiver: Cabletron Systems TPT
                                         10BASE-T
                                         Twisted Pair Transceiver

Type: 8 Pin RJ45 Jack (Figure A-1).
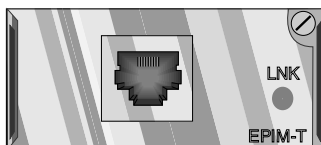
Figure A-1. EPIM-T (with RJ45 Port)

A slide switch on the EPIM-T determines the cross-over status of the cable pairs. The switch residing on the **X** side indicates the pairs internally cross over. If the switch resides on the **=** side, the pairs do not internally cross over. (See Figure A-2.)

Position X
(crossed over)

1. RX+   5. NC
2. RX-   6. TX-
3. TX+   7. NC
4. NC   8. NC

Position =
(not crossed over)

1. TX+   5. NC
2. TX-   6. RX-
3. RX+   7. NC
4. NC   8. NC
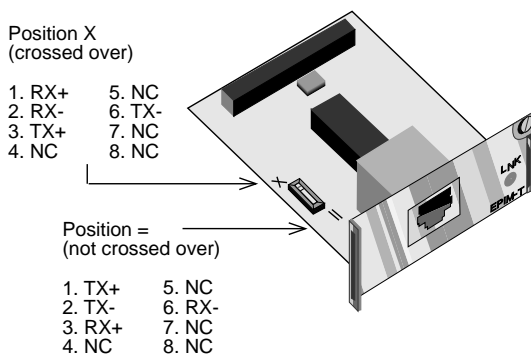
Figure A-2. Cross-over Switch on the EPIM-T

A.9   EPIM-F1/F2 (MULTIMODE FIBER OPTIC PORT)

Internal Transceiver: Cabletron Systems FOT-F
                                                        Fiber Optic Transceiver

Type:
    EPIM-F1:   SMA fiber optic ports (Figure A-3)
    EPIM-F2:   ST fiber optic ports (Figure A-3)
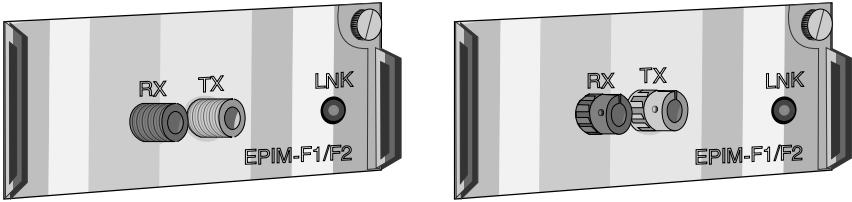
Figure A-3. EPIM-F1 and EPIM-F2

NOTE
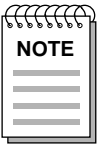
The transmitter power and receive sensitivity levels, below, represent Peak Power Levels after optical overshoot. You must use a Peak Power Meter to correctly compare the above values to those you measure on any particular port. If you measure Power Levels with an Average Power Meter, you must subtract 3 dBm from the measurement to correctly compare measured values to the values below (e.g., -29.5 dBm peak = -32.5 dBm average).

Table A-1, EPIM-F1/-F2 Statistics

Receive Sensitivity:	-29.5 dBm
Max Receive Power:	-8.2 dBm
Transmitter Power Into -	
50/125 µm fiber:	-13.0 dBm
62.5/125 µm fiber:	-10.0 dBm
100/140 µm fiber:	-7.0 dBm
Bit Error Rate:	Better than 10^{-10}

A.10   EPIM-F3 (SINGLE MODE FIBER OPTIC PORT)

Internal Transceiver: Cabletron Systems FOT-F3
                               Fiber Optic Transceiver

Type: ST fiber optic ports (Figure A-4)

Figure A-4. EPIM-F3

NOTE
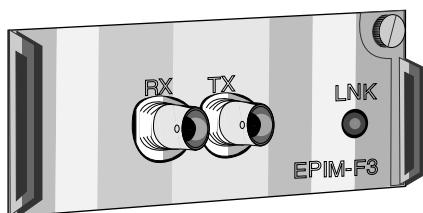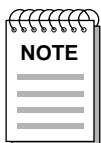
Transmitter power is inversely proportional to temperature rise. Use the Output Power Coefficient to calculate increased or decreased power output for your operating environment. For example, typical power output at 25C equals -16.4 dBm. For a 4C temperature increase, multiply the typical coefficient (-0.15 dBm) by four, and add the result to the typical output power (4 x -0.15 dBm + -16.4 dBm = -17.0 dBm).

Table A-2. EPIM-F3 Statistics

Parameter	Typical	Minimum	Maximum
Transmitter Peak Wave Length:	1300 nm	1270 nm	1330 nm
Spectral Width:	60 nm	—	100 nm
Rise Time:	3.0 ns	2.7 ns	5.0 ns
Fall Time:	2.5 ns	2.2 ns	5.0 ns
Duty Cycle:	50.1%	49.6%	50.7%
TX Power:	-15.1 dBm		
TX Budget:	14.4 dBm		
RX Sensitivity:	-29.5 dBm		
MAX Receive Power:	-6.99 dBm		
Bit Error Rate:	Better than 10^{-10}		

NOTE
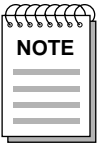
The above transmitter power levels and receive sensitivity levels represent Peak Power Levels after optical overshoot. You must use a Peak Power Meter to correctly compare the above values to those you measure on any particular port. If you measure Power Levels with an Average Power Meter, you must subtract 3 dBm from the measurement to correctly compare those measured values to the values listed above (e.g., -29.5 dBm peak = -32.5 dBm average).

A.11 EPIM-C (BNC PORT)

Internal Transceiver: Cabletron Systems TMS-3
                                         Transceiver

Type: BNC receptacle, with gold
                                         center contact, for use with BNC
                                         type T-connectors and RG-58
                                         thin-net cable (Figure A-5).
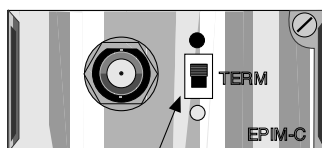
Internal Termination Switch
● = On (internally terminated)
○ = Off (need external termination)

Figure A-5. EPIM-C (with BNC Port)

Termination: Using the switch to the side of
                                         the port, you can internally
                                         terminate the port on the module
                                         via a built-in 50Ω terminator.
                                         This eliminates the need to
                                         connect the port to a T-connector
                                         and terminator.

Grounding: For safety, connect only one end
                                         of a thin-net segment to earth
                                         ground. Do not connect the BNC
                                         port of an EPIM-C to earth
                                         ground.

⚠ *Connecting a thin coaxial cable segment to earth ground at
more than one point can produce dangerous ground currents.*

A.12   EPIM-A AND EPIM-X (AUI PORT)

Interface Connector: DB-15 Port (female connector
                                        for EPIM-A, male connector for
                                        EPIM-X) (Figure A-6).

Type: 15 position D type receptacle
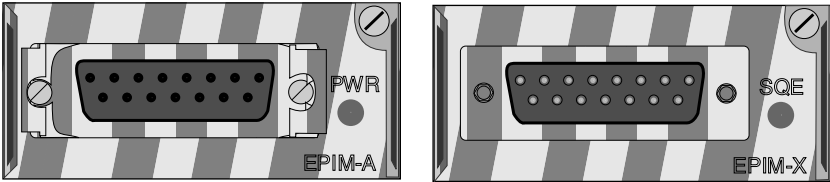
Figure A-6. EPIM-A and EPIM-X (AUI Port)

Table A-3. DB-15 Pinouts

Pin			Pin		
	1	Logic Ref.		9	Collision -
	2	Collision +		10	Transmit -
	3	Transmit +		11	Logic Ref.
	4	Logic Ref.		12	Receive -
	5	Receive +		13	Power (+12 Vdc)
	6	Power Return		14	Logic Ref.
	7	No Connection		15	No Connection
	8	Logic Ref.			

Connector Shell: Protective Ground

APPENDIX B

EMM-E6 OIDs

This Appendix contains a selected number of OID strings that are among
the most frequently needed. The OIDs are implemented by using either
the SNMP Tools procedures detailed in Chapter 9 or the MIB Navigator
procedures located in Chapter 13. Note that the OIDs can be accessed
using LANVIEW, SPECTRUM, SPMA, or the SNMP element
management packages of other vendors.

B.1 SPANNING TREE PROTOCOL

The following OID is used to select the desired Spanning Tree Protocol.

ctBridgeStpProtocolSpecification

> Description: This object allows the network manager to select
> which Spanning Tree Protocol will be operational on the bridge.
> The value 'decLb100' (2) indicates the DEC LANBridge 100
> Spanning Tree Protocol. The value 'ieee8021d' (3) indicates the
> IEEE 802.1d Spanning Tree Protocol. The value 'none' (1)
> indicates no Spanning Tree Protocol is operational.

> | | | |
> |---|---|---|
> | Object Identifier: | **1.3.6.1.4.1.52.4.1.2.3.2.1** | |
> | Data Type: | Integer | |
> | Values: | 1 | None |
> | | 2 | decLb100 |
> | | 3 | ieee8021 |
> | Access Policy: | read-write | |

B.2 CONFIGURING ARP REQUEST PACKETS

The EMM-E6's SNMP Tools Screen allows you to generate an Address Resolution Protocol (ARP) Request packet utilizing specific framing through local management. An ARP Request is used to send an SNMP Trap to a destination node that has not yet made or established contact with the EMM-E6. This situation may occur when the destination node in question has been moved from one port or channel interface of the EMM-E6 to another location and has not yet transmitted information which would notify the EMM-E6 of its network location. The generation of ARP Request packets in such a situation would allow the EMM-E6 to locate the reconfigured station without waiting for that station to transmit.

rptrScrAddrMgmtHashType

> Description: Forces the EMM-E6 to utilize a specific framing type for any ARP Request packet. The values entered determine the framing type utilized for the ARP packet. Please note that any changes to the framing type to be utilized for ARP requests will take effect after the next soft reset of the EMM-E6.

Object Identifier:	**1.3.6.1.4.1.52.4.2.2.2.3.1.2.2.2.1.1.1.8.1**	
Data Type:	Integer	
Values:	2	Ethernet Framing
	3	802.3=802.2 w/SNAP Header
Access Policy:	read-write	

B.3   PORT GROUP SECURITY

The next seven OIDs are used for port group security features.

rptrSrcAddrMgmtPortLock

Description: Setting this object to lock activates the network port security lock. Setting a value of portMisMatch (3) is invalid. A read of PortMisMatch means that the lock status between the port group, port and repeater levels do not agree.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.1.5.3.2**
Data Type: Integer
Values: 1   unlock
                    2   lock
                    3   portMisMatch
Access Policy: read-write

rptrPortGrpSrcAddrLock

Description: Allows the setting of the lock status for this port group. Unlock (1), unlocks the source address lock for this group. Lock (2) locks the source address for this group. Setting a value of portMisMatch (3) for this value is invalid. A read of PortMisMatch (3) means that the lock status for the ports within the port group does not match the lock status for the port group.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.2.6.1.2**
Data Type: Integer
Values: 1   unlock
                    2   lock
                    3   portMisMatch
Access policy: read-write

rptrPortSecurityLockStatus

Description: Defines the lock status for this particular port entry.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.3.9.1.1.3**
Data Type: Integer
Values: 1   unlock
                  2   lock
Access Policy: read-write

rptrPortSecurityLockAddAddress

Description: Setting a value to this object adds a new entry to the
rptrPortSecurityListTable. When read, this object displays an
Octet String of size 6 with each octet containing a 0. This object
provides an easy method to add or delete conceptual rows in the
rptrPortSecurityListTable. The returned value has little or no
actual meaning.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.3.9.1.1.4**
Data Type: Octet String (size 6)
Access Policy: read-write

rptrPortSecurityLockDelAddress

Description: Setting a value to this object deletes a corresponding
entry in the rptrPortSecurityListTable. When read, this object
returns the last deleted source address. An Octet String of size 0 is
returned if no objects were deleted since last system reset.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.3.9.1.1.5**
Data Type: Octet String
Access Policy: read-write

rptrPortSecurityDisableOnViolation

Description: Designates whether port is disabled if source address is violated. A source address violation occurs when an address is detected which is not in the source address list for this port. If this port is disabled for this port address violation it can be enabled by setting rptrPortMgmtAdminState. Default state is enabled (2).

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.9.1.1.6**	
Data Type:	Integer	
Values:	1	disable
	2	enable
Access Policy:	read-write	

rptrPortSecurityFullSecEnabled

Description: A port that is set to full security and is locked will scramble all packets, which are not contained in the expected source address list, including broadcasts and multicasts. A port that is set to partial security will allow broadcast and multicasts to repeat unscrambled. Default state disabled (1).

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.9.1.1.7**	
Data Type:	Integer	
Values:	1	disable
	2	enable
Access Policy:	read-write	

B.4   ENABLING & DISABLING SNMP TRAPS

The EMM-E6 supports the collection and reporting of SNMP Traps of several types and at several levels. SNMP Trap sending may be enabled or disabled for the following trap types: segmentation, link, and source addressing. The traps may be enabled on the network level, module level, or port level.

B.4.1   Enabling Network Level SNMP Traps

The next three OIDs control traps enable and disable at the network level or channel level.

rptrHwTrapsSetLink

Description: Enables and disables link traps for this network (i.e., Channel A, B, or C).

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.1.6.1.1**
Data Type: Integer
Values: 1   disable
                     2   enable
Access Policy: read-write

rptrHwTrapsSetSeg

Description: Enables and disables segmentation traps for this network (i.e., Channel A, B, or C).

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.1.6.1.2**
Data Type: Integer
Values: 1   disable
                     2   enable
Access Policy: read-write

rptrSaTrapSetScraddr

Description: Enables and disables source address traps for this
network (i.e., Channel A, B, or C).

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.1.6.2.1**
Data Type: Integer
Values: 1   disable
                      2   enable
Access Policy: read-write

B.4.2   Enabling Module Level SNMP Traps

The next three OIDs are for traps enable and disable at the board level.
The **<b#>** value is the number of the module in the MMAC chassis to be
examined. This number will be based on the location of the module in the
chassis. For detailed descriptions of the location numbering scheme in
your MMAC chassis, please refer to your MMAC User's Guide.

rptrPortGrpHwTrapSetLink

Description: Enables and disables link traps for the specified port
group at the board level.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.2.5.1.1.1.2.<b#>**
Data Type: Integer
Values: 1   disable
                      2   enable
Access Policy: read-write

rptrPortGrpHwTrapSetSeg

Description: Enables and disables segmentation traps for the specified port group at the board level.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.2.5.1.1.1.3.\<b#\>**
Data Type: Integer
Values: 1 disable
2 enable
Access Policy: read-write

rptrPortGrpSaTrapSetSrcaddr

Description: Enables and disables segmentation traps for the specified port group at the board level.

Object Identifier: **1.3.6.1.4.1.52.4.1.1.1.4.2.5.1.1.2.\<b#\>**
Data Type: Integer
Values: 1 disable
2 enable
Access Policy: read-write

B.4.3 Enabling Port Level SNMP Traps

The next three OIDs are for traps enable and disable at the port level. The \<b#\> value is the number of the module in the MMAC chassis to be examined. This number will be based on the location of the module in the chassis. For detailed descriptions of the location numbering scheme in your MMAC chassis, please refer to your MMAC User's Guide. Likewise, the \<p#\> value is the assigned number of the individual port on that module which SNMP Traps will be enabled or disabled for. Port numbers may be determined by examining the faceplate of the module, where they are clearly printed.

rptrPortHwTrapSetLink

Description: Enables and disables link traps for this port.

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.8.1.1.1.3.\<b#\>.\<p#\>**	
Data Type:	Integer	
Values:	1	disable
	2	enable
Access Policy:	read-write	

rptrPortHwTrapSetSeg

Description: Enables and disables segmentation traps for this port.

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.8.1.1.1.4.\<b#\>.\<p#\>**	
Data Type:	Integer	
Values:	1	disable
	2	enable
Access Policy:	read-write	

rptrPortGrpSaTrapSetSrcaddr

Description: Enables and disables source address traps for the specified port group.

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.8.2.1.1.3.\<b#\>.\<p#\>**	
Data Type:	Integer	
Values:	1	disable
	2	enable
Access Policy:	read-write	

B.5   ACTIVATING RMON GROUPS

The initial configuration of the EMM-E6 at installation does not provide
the activation of the RMON Default and Host Groups. These management
groups may be activated or deactivated through local management using
OID Sets. As the specific OID used to control each RMON bundle is
dependent upon the presence or absence of BRIMs and their type, an
SNMP Get is necessary to determine the OID instances of the RMON
bundles before they may be enabled or disabled.

chCompName

> Description: Returns OID values for the location of the RMON
> bundle OIDs in the device being examined. These values may be
> used in conjunction with the **chCompAdminStatus** OID (below)
> to activate and deactivate the individual RMON bundles.

> Object Identifier: **1.3.6.1.4.1.52.4.1.1.2.4.1.5**
> Data Type: Integer
> Access Policy: read-write

chCompAdminStatus

> Description: Enables and disables the RMON Default Group for
> an EMM-E6.

> Object Identifier: **[Result of above SNMP Get]**
> Data Type: Integer
> Values: 7   disable
>   3   enable
> Access Policy: read-write

B.6   BRIDGING

The following OID is used to enable and disable the interface for the bridging function.

dot1dstpPortEnable

Description: The enabled/disabled status of the port.

Object Identifier:	**1.3.6.1.2.1.17.2.15.1.4**	
Data Type:	Integer	
Values:	1	enable
	2	disable
Access Policy:	read-write	

B.7   TRUNK PORT SECURITY

The following OID is required if security is not desired on a trunk port. The user must force the port to be a trunk port before locking the port via the module or channel. Failing to do this will cause the port to become locked out when the third address is seen on the trunk port.

rptrPortSrcAddrForceTrunk

Description: When this object is set to Force, it places the port into a Trunk topology state whether or not the network traffic warrants such a state. When this object is set to NoForce, it allows the port to assume the topological state it would naturally assume based on the network activity across it. When read, this object reports the current setting.

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.3.5.1.4**	
Data Type:	Integer	
Values:	1	NoForce
	2	Force
Access Policy:	read-write	

B.8 CHANNEL SELECTION

The following two OIDs are needed to select channel assignments (A, B, or C) for all boards or individual ports. These OIDs are needed for products supporting multichannel connectivity.

fnbconnect

> Description: Denotes the connection status of the CSMA/CD board to the inter-RIC bus.

Object Identifier:	**1.3.6.1.4.1.52.1.6.1.2.2.1.1.2.slot**	
Data Type:	Integer	
Values:	1	Channel B
	2	Channel C
	4	Channel A
Access Policy:	read-write	

fnbPortConnectPortAssignment

> Description: Provides the capability to change or query the specific interface that the port is assigned.

Object Identifier:	**1.3.6.1.4.1.52.1.6.1.2.3.1.1.3.slot.port**	
Data Type:	Integer	
Values:	1	Channel A
	2	Channel B
	3	Channel C
Access Policy:	read-write	

B.9   OID HASHING ON SOURCE ADDRESES

The following OID allows the enabling and disabling of DEC hashing, which may be necessary or desired in DECnet and mixed IEEE 802.3/DECnet environments.

rptrSrcAddrMgmtHashType

Description: This enables and disables DECnet hashing on source addresses which is useful in DECnet environments.

Object Identifier:	**1.3.6.1.4.1.52.4.1.1.1.4.1.5.3.4.0**	
Data Type:	Integer	
Values:	1	NoDECnetHashing
	2	DECnetHashing
Access Policy:	read-write	

B.10   REMOTE DOWNLOADING

For detailed step-by-step instructions on the use of OIDs for forcing a remote download of firmware instruction code to the EMM-E6, please refer to **Image File Download**, Chapter 15 of the main text.

GLOSSARY

This glossary provides brief descriptions of some of the recurrent terms in the main text, as well as related terms used in discussions of the relevant networking discussions. These descriptions are not intended to be comprehensive discussions of the subject matter. For further clarification of these terms, you may wish to refer to the treatments of these terms in the main text.

Words in the glossary description text listed in boldface type indicate other entries in the glossary which may be referred to for further clarification.

10BASE-2   **IEEE** standard which governs the operation of devices connecting to Ethernet thin **coaxial** cable.

10BASE-FL   **IEEE** standard which governs the operation of devices connecting to Ethernet **fiber optic** cable. Supersedes previous FOIRL standard.

10BASE-T   **IEEE** standard which governs the operation of devices connecting to Ethernet Unshielded Twisted Pair (**UTP**) cable.

Alarm   A notification, generated by the operation of **SNMP**, which is sent to a management station to indicate a problem with the network or warn of an error condition.

Application   1: A software operation performed by a workstation or other network **node**. 2: A layer of the **OSI Model**.

Architecture   A collective rule set for the operation of a network. Architectures describe the means by which nodes transmit and receive information in the network. See also: **Ethernet, Topology**.

ATM   Asynchronous Transfer Mode. A networking **architecture** that is based on the use of connections between communicating devices that are set up, used, and then eliminated.

Attenuation	Loss of signal power (measured in decibels) due to transmission through a cable. Attenuation is dependent on the type, manufacture and installation quality of cabling, and is expressed in units of loss per length, most often dB/m.
AUI	Attachment Unit Interface. A cabling type used in Ethernet networks, designed to connect network stations and devices to **transceivers**.
Backbone	A portion of a network which provides the interconnection of a number of separate, smaller networks.
Backplane	The portion of a **modular chassis** to which all **modules** are connected. Typically the backplane provide power and management functions to each module, and is used to provide networking connections, via **buses**, to all modules in the modular chassis.
Bit	Binary Digit. A bit is the smallest unit of information, consisting of a single binary number. A bit is represented by a numerical value of 1 or 0.
BOOTP	Bootstrap Protocol. Checks **MIB** variables of a **SNMP** manageable device to determine to determine wether it should start up using its existing **firmware** or boot up from a network **server** specifically configured for the purpose.
Branch Group	A collection of **MIB**s related by common function. These MIBs are collected into families called branches. See also **Leaf Object, MIB Tree**.
Bridge	Bridges are network devices which connect two or more separate network segments while allowing traffic to be passed between the separate networks when necessary. Bridges read in packets and decide to either retransmit them or block them based on the destination to which the packets are addressed.
BRIM	Bridge/Router Interface Module. BRIMs are added to BRIM-capable Cabletron equipment to provide connections to external networks through an integrated **bridge** or **router**.

Broadcast	A type of network transmission; a broadcast transmission is one which is sent to every station on the network, regardless of location, identification, or address.
Buses	Physical portions of the **backplane** of a modular chassis which pass information between **modules**.
Card	See **Module**.
Channel	A portion of a backplane **bus** which is specifically partitioned off for the transmission of one type of network data.
Chassis	See **Modular Chassis**.
Client	A workstation or node which obtains services from a **server** device located on the network.
Client-Server	A computing model which is based on the use of dedicated devices (**servers**) for the performance of specific computational or networking tasks. These servers are accessed by several **clients**, workstations which cannot perform those functions to the same extent or with the same efficiency as the servers.
Coaxial	An Ethernet **media** type which consists of a core of electrically conductive material surrounded by several layers of insulation and shielding.
Community Name	An identification which allows a specific level of access to the network device. Similar to a password, a Community Name acts to restrict access to control capabilities and network statistics.
Concentrator	A network device which allows multiple network ports in one location to share one physical interface to the network.
Congestion	An estimation or measure of the utilization of a network, typically expressed as a percentage of theoretical maximum utilization of the network.
Connectivity	The physical connection of cabling or other **media** to network devices. The coupling of media to the network.

Console   See **Terminal**.

Cross-Over   A length of multi-stranded cable in which the transmit
                     wire(s) of one end is/are crossed over within the cable to
                     connect to the receive wire(s) of the other end. Cross-
                     Overs are used to connect devices to like devices, ensuring
                     that transmit and receive connections are properly made.

Crosstalk   A corruption of the electrical signal transmitted through a
                     Shielded or Unshielded twisted pair cable. Crosstalk refers
                     to signals on one strand or set of strands affecting signals
                     on another strand or set of strands.

CSMA/CD   Carrier Sense Multiple Access with Collision Detection.
                     CSMA/CD is the basis for the operation of **Ethernet**
                     networks. CSMA/CD is the method by which stations
                     monitor the network, determine when to transmit data, and
                     what to do if they sense a **collision** or other error during
                     that transmission.

Data   Information, typically in the form of a series of **bits**, which
                     is intended to be stored, altered, displayed, transmitted, or
                     processed.

Data Loop   A condition caused by the creation of duplicate paths
                     which network transmissions could follow. Data loops are
                     created by the use of redundant connections between
                     network segments or devices. Ethernet networks cannot
                     effectively function with data loops present. To allow the
                     creation of fault-tolerant networks, data loops are
                     automatically detected and eliminated by the **Spanning
                     Tree** algorithm.

DB15   A 15-pin connector used to terminate **transceiver** cables
                     in accordance with the **AUI** specification.

DB9   A 9-pin connector, typically used in Token Ring networks
                     and for serial communications between computers.

Decryption   The translation of data from an **encrypted** form into a
                     form both recognizable and utilizable by a workstation,
                     node, or network **device**.

Dedicated   Assigned to one purpose or function.

Default   the IP address of the network or host to which all packets
Gateway   addressed to unknown network or host are sent

Device   Any discrete electronic item connected to a network which
(network)   either transmits and receives information through it,
                       facilitates that transmission and reception, or monitors the
                       operation of the network directly.

DLM   Distributed LAN Monitor. DLM is a feature of some
                       SNMP management devices which allows that device to
                       locally monitor other devices under its control and report
                       to a central network management station any noted errors.
                       This frees the network management station from directly
                       monitoring every SNMP device.

DNI   Desktop Network Interface. DNI cards are devices which
                       are added to workstations to provide them with a
                       connection to a network (NIC).

EEPROM   Electronic Erasable Programmable Read-Only Memory.

Encryption   A security process which encodes raw data into a form that
                       cannot be utilized or read without **decryption**.

EPIM   **Ethernet Port** Interface Module. EPIMs are added to
                       specifically-designed slots in Cabletron Ethernet products
                       to provide connections to external **media**. EPIMs allow a
                       great flexibility in the media used to connect to networks.

Ethernet   A networking **architecture** which allows any station on
                       the network to transmit at any time, provided it has
                       checked the network for existing traffic, waited for the
                       network to be free, and checked to ensure the transmission
                       did not suffer a **collision** with another transmission.See
                       also **CSMA/CD**.

Fault-   The ability of a design (device or network) to operate at
Tolerance   full or reduced capacity after suffering a failure of some
                       essential component or connection. See also **redundant**.

FDDI	Fiber Distributed Data Interface. A high-speed networking **architecture**. FDDI requires that stations only transmit data when they have been given permission by the operation of the network, and dictates that stations will receive information at pre-determined intervals. See also **Token**.
Fiber optics	Network **media** made of thin filaments of glass surrounded by a plastic cladding. Fiber optics transmit and receive information in the form of pulses of light. See **multimode** and **single mode**.
File	A collection of related **data**.
Fileserver	A network **server** device which stores and maintains data files for the use and modification of users on the network.
Firmware	The software instructions which allow a network device to function. See also **Image file**.
Flash EEPROM	See **EEPROM**.
FNB	Flexible Network Bus. A Cabletron **backplane** design which enables an FNB-configured chassis to support multiple network **architectures** simultaneously.
Frame	A group of **bits** that form a discrete block of information. Frames contain network control information. The size and composition of a frame is determined by the network **protocol** being used.
Gateway	A **router**.
Heartbeat	See **SQE**.
Hexadecimal	A base 16 numerical system. Digits in hexadecimal run from 0 to 9 and continue from A to F, where F is equivalent to the decimal number 16.
Host	A device which acts as the source or destination of data on the network.

Hot Swap   Hot Swap capability indicates that a product is capable of being removed from an operating **modular chassis** and reinserted or replaced without requiring that the chassis and all associated modules be powered down.

Hub   See **Modular Chassis**.

IANA   **Internet** Assigned Numbers Authority. An agency which assigns and distributes **IP addresses**.

IEEE   Institute of Electrical and Electronic Engineers. A standards-making body.

IETF   Internet Engineering Task Force. A standards-making body.

Image File   Software instruction code which is downloaded to an intelligent network device. See also **Firmware**.

Impedance   A measure of the opposition of electrical current or signal flow in a length of cable.

In-Band   Performed through the operating network architecture. Refers most commonly to management functions. See also **Out-of-Band**.

Interface   A connection to a network. Unlike a **port**, an interface is not necessarily an available physical connector accessible through the front panel of a device. Interfaces may be used as backplane connections, or may be found only in the internal operation of a module (All ports are interfaces, but not all interfaces are ports).

Internet   A world-wide network which provides access through a vast chain of private and public LANs.

Inter-operability   The capacity to function in conjunction with other devices. Used primarily to indicate the ability of different vendors' networking products to work together cohesively.

IP   Internet Protocol.

IP Address   Internet Protocol address. The IP address is associated, by the network manager or network designer, to a specific **interface**. The availability of IP addresses is controlled by the **IANA**.

ISO   International Organization for Standardization. The ISO has developed a standard model on which network operation is based, called the **OSI Model**.

Jitter   Degradation of network signals due to a loss of synchronization of the electrical signals. Jitter is often a result of passing a signal through too many **repeaters**.

LAN   Local Area Network.

LANVIEW   A system which relates diagnostic, troubleshooting, and operational information pertaining to network **devices** through the use of prominently displayed **LED**s.

LDRAM   Local Dynamic Random Access Memory

Leaf Object   An end unit in a **MIB tree**. Leaf objects are accessed through a series of **branch groups**. Leaf objects are always individual **MIB**s.

LED   Light Emitting Diode. A simple electronic light, used in networking equipment to provide diagnostic indicators. Also used as a light source for some **fiber optic** communications equipment.

Load   An indication of network utilization.

MAC Address   Media Access Control address. The MAC address is associated, usually at manufacture, with a specific **interface**.

Mbps   Megabits Per Second. Mbps indicates the number of groups of 1000 **bits** of data that are being transmitted through an operating network. Mbps can be roughly assessed as a measure of the operational "speed" of the network.

Media	Physical cabling or other method of interconnection through which network signals are transmitted and received.
MIB	Management Information Base. A database of data related to a specific management or manageable network device, which may be viewed or modified through **SNMP** commands.
MIB Tree	The MIB Tree is the collection of all **MIB**s that can be used to monitor or control a network device. MIB Trees are made up of several **branch groups** which lead to **leaf objects**, or MIBs.
Micron (μ)	A micrometer, one millionth of a meter.
MIM	Media Interface Module. See also: **Module**.
Mission-Critical	Vital to the operation of a network, company, or agency.
Modular Chassis	A device which provides power, cooling, interconnection, and monitoring functions to a series of flexible and centralized **modules** for the purposes of creating a network or networks.
Module	A discrete device which is placed in a **modular chassis** to provide functionality which may include, but is not limited to; bridging, routing, connectivity, and repeating. Modules are easily installed and removed. Also, any device designed to be placed in another device in order to operate. See also: **BRIM, EPIM**.
Multichannel	A Cabletron Ethernet design which provides three separate network channels (of Ethernet or Token Ring architecture) through the backplane of a chassis, allowing for the creation of multiple networks in a single chassis.
Multimode	A type of **fiber optics** in which light travels in multiple modes, or wavelengths. Signals in Multimode fiber optics are typically driven by **LED**s.
Nanometer	One billionth of a meter.

Node   Any single end station on a network capable of receiving, processing, and transmitting packets.

NVRAM   Non-Volatile Random Access Memory. Memory which is protected from elimination during shutdown and between periods of activity, frequently through the use of batteries.

Octet   A numerical value made up of eight binary places (**bits**). Octets can represent decimal numbers from zero (0000 0000) to 255 (1111 1111).

OID   Object Identifier.

OSI Model   Open Standards Interconnect. A model of the way in which network communications should proceed from the user process to the physical media and back.

Out-Of-Band   Performed without requiring the operation of the network architecture. Most commonly used in reference to local management operations.

Packet   A discrete collection of **bits** that form a block of information. Packets are similar to **frames**, but may be made up of control information (frames) or data to be transmitted.

Plenum   A cabling term which indicates a cable with insulating material that is considered safe to use in return-air plenum spaces (in contrast to PVC insulation) due to its low relative toxicity if ignited.

Port   A physical connector which is used as an interface to cabling with modular or pinned connectors. Ports are associated with **Interfaces**.

Port Assignment The association, through software management, of specific **ports** on a network device to specific **channels** of a **backplane**. This assignment is done on an individual port basis.

Protocol   A set of rules governing the flow of information within a communications infrastructure. Protocols control operations such as **frame** format, timing, and error correction. See also **Architecture**.

PVC   Polyvinyl Chloride. A material commonly used in the fabrication of cable insulation. This term is used to describe a non-plenum rated insulating material. See also **Plenum**.

Redundant   Extra or contingent. A redundant system is one that is held in reserve until an occurrence such as a failure of the primary system causes it to be required.

Repeater   A network device consisting of a receiver and transmitter which is used to regenerate a network signal to increase the distance it may traverse.

RJ45   A modular connector style used with twisted pair cabling. The RJ45 connector resembles the modern home telephone connector (RJ11).

RMIM   Repeating Media Interface Module. A term used to indicate a family of Cabletron Ethernet Media Interface Modules (See **MIM**) which are capable of performing their own repeater functions.

RMON   Remote MONitoring. RMON is a network management standard which provides more detailed network information and status reporting than **SNMP**.

Router   A router is a device which connects two or more different network segments, but allows information to flow between then when necessary. The router, unlike a **bridge**, examines the data contained in every packet it receives for more detailed information. Based on this information, the router decides wether to block the packet from the rest of the network or transmit it, and will attempt to send the packet by the most efficient path through the network.

SDRAM   Shared Dynamic Random Access Memory.

Segment   A portion of a network which is separated from other networks. A segment may be one portion of a bridged, switched, or routed network. Segments must be capable of operating as their own networks, without requiring the services of other portions of the network.

Server   A workstation or host device that performs services for other devices (**clients**) on the network.

SIMM   Single In-line Memory Module. A collection of Random Access Memory microprocessors which are placed on a single, replaceable printed circuit board. These SIMMs may be added to some devices to expand the capacity of certain types of memory.

Single Mode   A type of **fiber optics** in which light travels in one predefined mode, or wavelength. Signals in single mode fiber optics are typically driven by lasers. The use of lasers and the transmission characteristics of single mode fiber optics allow the media to cover greater distances than **multimode** fiber optics.

SMA   Sub-Miniature Assembly. A modular connector and port system used in **multimode** fiber optic cabling. The SMA connector is threaded, and is screwed into an SMA port.

SNMP   Simple Network Management Protocol. SNMP is a standardized set of network monitoring tools. See also **RMON**.

Spanning Tree   A mathematical comparison and decision algorithm performed by Ethernet bridges at power-up. Spanning tree detects the presence of data loops and allows the bridges to selectively activate some ports while others remain in a standby condition, avoiding the data loops and providing redundant paths in the event of bridge failures.

SQE   Signal Quality Error. A self-monitoring test performed by some Ethernet equipment which examines the status of the device's connection to the network at arbitrary and predefined intervals.

ST　　　　　　Straight-Tip. A modular connector and port system used with both **multimode** and **single mode** fiber optic cabling. The ST connector utilizes an insert and twist-lock mechanism.

Station　　　　See **node**.

STP　　　　　Shielded Twisted Pair. Refers to a type of cabling, most commonly used in Token Ring networks, which consists of several strands of cables surrounded by foil shielding, which are twisted together. See also **UTP**.

Straight-Through　　A length of multi-stranded cable in which the transmit wire(s) of one end is/are passed directly through the cable to the same location on the other end. Straight-through cables are used for most facility cabling. See also **cross-over**.

Subnet　　　　A physical network within an **IP** network.

Subnet Mask　　A 32-**bit** quantity which may be set up in **SNMP** management devices to indicate which bits in an **IP address** identify the physical network.

Switch　　　　A network device which connects two or more separate network segments and allows traffic to be passed between them when necessary. A switch determines if a **packet** should be blocked or transmitted based on the destination address contained in that packet.

TCP　　　　　Transmission Control Protocol.

Terminal　　　A device for displaying information and relaying communications. Terminals do not perform any processing of data, but instead access processing-capable systems and allow users to control that system.

Throughput　　The rate at which discrete quantities of information (typically measured in **Mbps**) are received by or transmitted through a specific device.

Token   A particular type of frame which informs a station in the **Token Ring** and **FDDI** network architectures that it may transmit data for a specified length of time. Once that time has expired, the station must stop transmitting and pass the token along to the next station in the network.

Token Ring   A network architecture which requires that stations only transmit data when they have been given permission by the reception of a **Token**, and dictates that stations will receive information at pre-determined intervals and in a definite series.

Topology   The physical organization of stations and devices into a network.

Transceiver   A device which transmits and receives. A transceiver provides the electrical or optical interface to the network media, and may convert signals from one media for use by another.

Trap   See **Alarm.**

User   Any person who utilizes a workstation or node on the network. Anyone who will complain if the network is not operating.

UTP   Unshielded Twisted Pair. A type of network media which consists of a number of individual insulated cable strands which are twisted together in pairs.

INDEX

LANVIEW LEDs

EMM-E6

SN

RESET ○

CPU ○

D C B A
STBY ○ ○ ○ ○
RCV ○ ○ ○ ○
XMT ○ ○ ○ ○
CLN ○ ○ ○ ○

BRIM-A100

| LED	DESCRIPTION
CPU	Flashing Green: Board Operating Properly. Red: CPU error condition.
STBY A, B, C, D	Amber indicates port or interface placed in standby state.
RCV A, B, C, D	Green indicates valid link from station to EMM-E6 interface. Amber indicates segment receiving traffic.
XMT A, B, C, D	Green indicates segment is transmitting traffic. Flashing red indicates port in standby due to spanning tree operation.
CLN A, B, C, D	Red indicates collision detected on segment. Occasional activation of CLN LED is normal.

SWITCH SETTINGS

Switch	Function
1	Cabletron Systems Use Only. Must be in **OFF** position.
2	Cabletron Systems Use Only. Must be in **OFF** position.
3	Cabletron Systems Use Only. Must be in **OFF** position.
4	MIMREV. Should be **OFF** unless THN-MIM s with part numbers below 9000043-05 are located in the MMAC.
5	Baud Rate Default. Sets local management console port baud rate. **OFF** (default) = 9600 Baud, **ON** = 2400 baud.
6	Forced Download. When toggled, forces image files to be loaded from BOOTP server by clearing information from NVRAM.
7	NVRAM Reset. When toggled, deletes user parameters stored in NVRAM and returns these parameters to factory default settings.
8	Password Default. When toggled, deletes user defined passwords stored in NVRAM and returns these passwords to factory default settings (public or [Return]).

INSTALLATION

- Slide the EMM-E6 into the first and second slots of the MMAC chassis (as shown below).
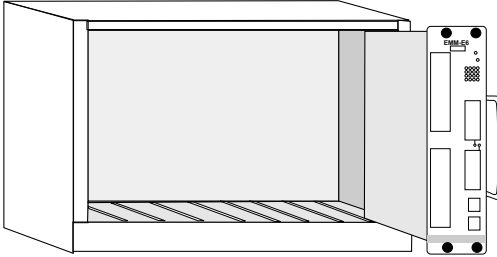
- Secure the module by tightening the knurled knobs at the top and bottom of the module.
- Power on the MMAC chassis. Monitor the state of the CPU LED.
- The CPU LED will flash, indicating the EMM-E6 is in boot state. During this period, which may last up to 5 minutes, the STBY LEDs will blink to indicate the module's boot state.
- Fully operational EMM-E6 should display the following LED states:
    - CPU LED flashing, indicating normal operation.
    - STBY LEDs lit or unlit, depending on the results of spanning tree operation.
    - Appropriate BRIM/EPIM LEDs lit.
    - ON LED lit for the active Channel D EPIM.

TERMINAL SETUP

Use the following setup parameters for a VT Terminal or Terminal Emulation package to connect to Local Management functions.

Columns:	**80 Columns**	Controls:	**Interpret Controls**	Autowrap:	**No Autowrap**
Scroll:	**Jump Scroll**	Text Cursor:	**Cursor**	Cursor Style:	**Underline**
Mode:	**VT300, 7 Bit**	ID Number:	**VT320 or VT100**	Cursor Keys:	**Normal**
Transmit:	**9600**	Receive:	**9600**	XOFF:	**XOFF at 64**
Bits:	**8 Bits**	Parity:	**No Parity**	Stop Bit:	**1 Stop Bit**
Local Echo:	**No Local Echo**	Port:	**DEC-423**	Auto Answerback:	**No Auto Answerback**
Keys:	**Typewriter Keys**	Margin Bell:	**Margin Bell**	Warning Bell:	**Warning Bell**

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com