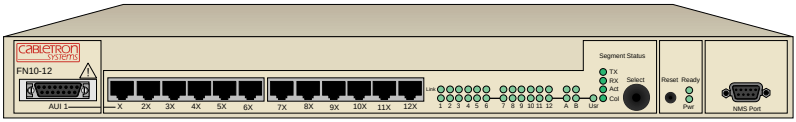
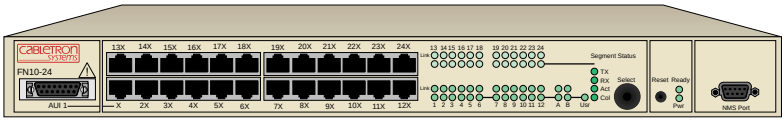
FAST NETWORK 10
USER GUIDE





CABLETRON SYSTEMS

The Complete Networking Solution™

NOTICE

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Order Number: 9031805-01 May 1996

Printed on  Recycled Paper

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

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

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

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

EXCLUSION OF WARRANTY AND DISCLAIMER OF LIABILITY

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

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

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

UNITED STATES GOVERNMENT RESTRICTED RIGHTS

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

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

CONTENTS

CHAPTER 3 CONFIGURING YOUR FN10

CHAPTER 4 MONITORING AND MANAGING YOUR FN10

APPENDIX A TECHNICAL SPECIFICATIONS

CHAPTER 1
INTRODUCTION

1.1 ABOUT THIS MANUAL

This manual is for system administrators responsible for configuring, monitoring, and maintaining the Fast Network 10 (FN10). You should have a familiarity with networking concepts and principles. In addition, a basic understanding of SNMP is helpful.

Some FN10 configurations can only be done using an SNMP-based Network Management System (NMS). Therefore, how you configure and manage the FN10 is dependent on the NMS you use. Where applicable, this manual provides instructions for using the Local Console Manager (LCM) to perform basic configuration. Where it is not possible to use LCM, general instructions and guidelines applicable to most NMSs are provided.

The contents of each chapter are described below.

- Chapter 1, **Introduction**, outlines the contents of this manual and provides an overview of the FN10's switching functions and the Local Console Manager (LCM).
- Chapter 2, **Unpacking and Installing Your FN10**, describes the FN10 front and rear panels, how to install the FN10, how to connect the Local Console Manager (LCM), and how to connect the FN10 to the network.
- Chapter 3, **Configuring Your FN10**, provides instructions for configuring the FN10 using the Local Console Manager (LCM). It also provides some common Management Information Base (MIB) variables you may want to change.
- Chapter 4, **Monitoring and Managing Your FN10**, describes how to monitor FN10 status and statistics. It also describes how to manage the FN10 Ethernet ports using the Local Console Manager (LCM).

- Chapter 5, **FN10 Filters**, describes FN10 filtering and provides specific examples of how filters can be used. It also provides instructions for adding, modifying, and deleting Port filters using the Local Console Manager (LCM).
- Chapter 6, **FN10 Diagnostics and Troubleshooting**, describes the FN10 diagnostics and provides information on troubleshooting common problems.
- Appendix A, **Technical Specifications**, provides the FN10 specifications and basic 10BASE-T cabling pin assignments.
- Appendix B, **Glossary**, provides a glossary of terms both specific to the FN10 and common to the networking field.

1.2 GETTING HELP

If you need additional support related to the FN10, or if you have any questions, comments, or suggestions concerning this manual, contact Cabletron Systems Technical Support:

By phone	(603) 332-9400 Monday-Friday; 8 A.M. – 8 P.M. Eastern Time
By CompuServe	GO CTRON from any ! prompt
By Internet mail	support@ctron.com
By FTP	ctron.com (134.141.197.25)
Login	*anonymous*
Password	*your email address*

1.3 DOCUMENT CONVENTIONS

The following conventions are used throughout this document:

LCM commands, prompts, and information displayed by the computer appear in Courier typeface, for example:

```
Current Number of Learned Addresses: 133
Number of Defined Filters: 4
```

Information that you enter appears in Courier bold typeface, for example:

```
FN10 >status
```

Information that you need to enter with a command is enclosed in angle brackets < >. For example, you must enter a port number and an IP address to execute the `ipaddr <port #> <IP address>` command:

```
FN10 >ipaddr 6 192.138.217.40
```

Field value options appear in bold typeface. For example, a FN10 filter type can be either **Entry** or **Exit**.

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

Tip symbol. Conveys helpful hints concerning procedures or actions.

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

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

1.4 RELATED DOCUMENTATION

The following documentation may assist the user in using this product:

- *Fast Network 10 MIB Reference Guide* – contains enterprise MIB information.
- *Interconnections, Bridges and Routers,* Radia Perlman, Addison Wesley © 1992.
- *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (2nd edition), Volumes I and II, Douglas Comer, Prentice Hall © 1991.
- *The Simple Book, An Introduction to Management of TCP/IP-based internets*, Marshall T. Rose, Prentice Hall © Second Edition, 1994.

1.5 OVERVIEW

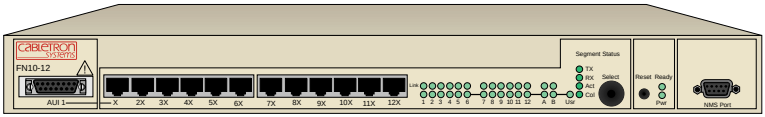
The FN10 is an intelligent Ethernet-to-Ethernet switch that is available in the following configuration options:

- **12 port** - 12 IEEE 802.3 10BASE-T Ethernet ports, including one Ethernet Attachment Unit Interface (AUI) connection.
- **12 port with FE up-link option** - 2 Fast Ethernet ports (100 Mbps) and 12 IEEE 802.3 10BASE-T Ethernet ports (10 Mbps), including one Ethernet Attachment Unit Interface (AUI) connection.
- **24 port** - 24 IEEE 802.3 10BASE-T Ethernet ports, including one Ethernet Attachment Unit Interface (AUI) connection.
- **24 port with FE up-link option** - 2 Fast Ethernet ports (100 Mbps), and 24 IEEE 802.3 10BASE-T Ethernet ports (10 Mbps), including one Ethernet Attachment Unit Interface (AUI) connection.

In addition, each FN10 configuration includes an RS232C port for out-of-band management.

The following figures show the different front panels for the 12 and 24 port FN10 configurations, and the rear panel for the optional 2 Fast Ethernet ports.

Front Panel with 12 10BASE-T (10 Mbps) Ports



Front Panel with 24 10BASE-T (10 Mbps) Ports

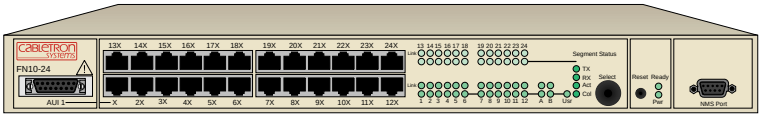


Figure 1-1 FN10 Front Panels

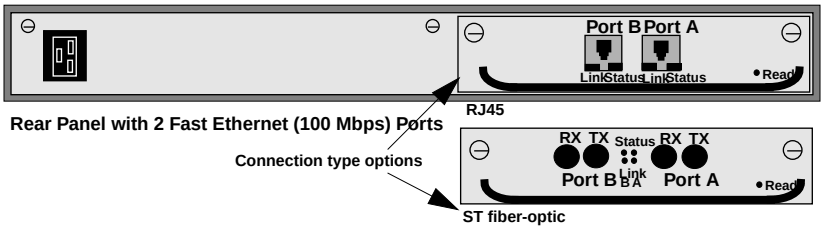


Figure 1-2 FN10 Rear Panel with the Optional Fast Ethernet Ports

The FN10:

- Provides dedicated bandwidth for each network connected to its ports.
- Provides full store and forward bridging functionality.
- Provides complete error checking functionality.
- Provides port trunking to increase bandwidth.
- Allows you to define virtual workgroups to optimize network traffic.
- Filters and forwards received Ethernet packets based on Network Management System (NMS) configurable parameters.
- Supports 48-bit IEEE 802 MAC addressing.

- Implements the Spanning Tree protocol (802.1d).
- Configured with factory-set defaults for immediate plug-and-play capability.

In addition, the FN10 offers features that can help you manage and maintain your network, such as:

- Configuration and management using the Simple Network Management Protocol (SNMP) with either an in-band or out-of-band connection.
- Protection against multicast storms.
- Data flow control based on user-defined data packet filters.
- Ability to define virtual workgroups for more efficient bandwidth usage.
- Compilation of statistics for traffic generated by each user device connected to a FN10 segment.
- Real time "what-if" analysis of the traffic flow throughout the network.

1.5.1 FN10 Architecture

The FN10 enables you to link two or more Local Area Networks (LANs) together. To accomplish this, the FN10 regulates network traffic on the basis of the source and destination addresses that are in each data packet it receives.

The FN10 is protocol-transparent, meaning it can handle different types of network traffic regardless of the network protocol, such as IP and IPX. As the FN10 reads addresses from the packets it processes, it builds a dynamic database of addresses called the *Bridge Address Table*. In this way, the FN10 continuously learns the addresses of all connected devices. Consequently, you can add new devices to the network, change device addresses, and remove devices from the network without having to reconfigure the FN10.

The Open System Interconnection (OSI) Reference Model, developed by the International Standards Organization (ISO), identifies the levels of functionality inherent in each of its seven layers. The FN10 operates at the

Media Access Control (MAC) sub-layer of the Data Link layer. Figure 1-3 shows the OSI Reference Model.

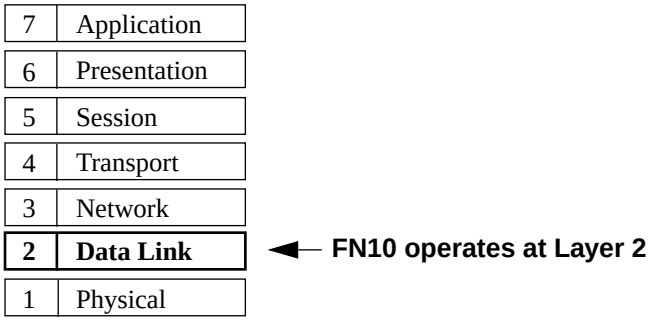


Figure 1-3 OSI Reference Model

Because the FN10 does not process any Network Layer information, it provides a high level of performance in terms of packet throughput. In addition, the FN10 does not need to learn network topology, requiring less programming and configuration time.

1.5.1.1 Store and Forward Switching

As an intelligent Ethernet switch, the FN10 uses full store and forward switching. Store and forward switching allows the FN10 to temporarily store packets until network resources, typically an unused link, are available for forwarding. This allows for complete error checking, and limits the amount of time between when a device requests access to the network and when it is granted permission to transmit. In addition, full store and forward switching ensures data integrity, thus preventing network error conditions from being generated throughout the network.

1.5.1.2 Discarding Local Traffic

The FN10 checks all incoming packets for their destination address against the Bridge Address Table. If a packet's destination address is not on the same network segment as the originating packet, the FN10

forwards the packet to the network segment associated with that destination address. However, if the packet's source and destination address are on the same network segment, known as *local traffic*, the packet is automatically discarded (i.e., ignored by the FN10).

For example, a file transmitted from Workstation A to Workstation C in Figure 1-4 does not need to leave LAN 1. The FN10 connected to LANs 1 and 2 sees all traffic from LAN 1, including LAN 1 local traffic.

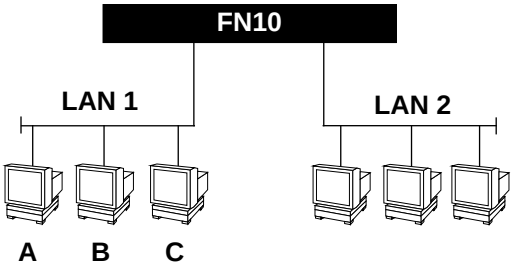


Figure 1-4 Typical Switching Application

By forwarding only packets addressed to devices on other network segments, the FN10 reduces unnecessary traffic and thereby enhances the overall performance of the network.

1.5.1.3 Spanning Tree Algorithm

The FN10 supports the IEEE 802.1d Spanning Tree algorithm. The Spanning Tree algorithm converts multiple LANs into a "spanning tree" of networks. It is used to prevent bridging loops. This standard defines a logical (not physical) network configuration consisting of one extended LAN without active duplicate paths between spanning tree bridges.

The FN10, along with other IEEE 802.1d Spanning Tree compliant bridges in the network, dynamically configure the network topology into a single Spanning Tree by exchanging Bridge Protocol Data Units (BPDUs). Typically, each LAN segment is sent one BPDU every two seconds.

When there are multiple FN10s connecting LANs in a loop, the Spanning Tree algorithm determines which FN10 should forward packets to the LAN. If there is a cable break or a port failure, the network topology is

automatically reconfigured by the Spanning Tree protocol to create an alternate path to the LAN.

1.5.2 FN10 Bridge Address Table

The FN10 creates and maintains a dynamic database of addresses called the Bridge Address Table. The FN10 examines every packet to determine its source address and LAN segment origin. It then compares the source address and segment information it finds to the entries in the Bridge Address Table.

If a packet's address is not already stored in the Bridge Address Table, the FN10 adds the learned address, associated segment number, and a timer value that indicates the age of the observation. Consequently, the FN10 knows the address and associated segment number the next time it sees that address. By using the information stored in the Bridge Address Table, the FN10 is able to quickly forward each packet to the correct LAN segment.

The FN10 learns addresses from all packets, including data transmissions and "keep alive" packets (packets sent by an idle station to let other stations know it is present and functional). When devices are added to the network, removed from it, or relocated, you do not have to reconfigure the FN10. The FN10 automatically learns new device addresses, recognizes when a previously used address is missing, or when a device has been moved to a new LAN segment.

An address stored in the Bridge Address Table is discarded if there is no subsequent activity from that address after a configured length of time (five minutes by default). This aging process ensures that the Bridge Address Table is continually updated.

Typically, addresses are continually added to and deleted from the Bridge Address Table, reflecting the dynamic nature of internetwork traffic. However, you can change an address from dynamic to static if you do not want the entry in the Bridge Address Table to get discarded.

Each dynamic entry includes:

- An Ethernet MAC address

- A single port number of the LAN on which the address resides
- The age of the entry
- Various statistics counters
- Any filtering restrictions added by a Network Management Station (NMS)

Each static entry contains the same information as a dynamic entry, except the static entry is not aged, and can contain a range of port numbers, rather than a single port number.

The FN10 stores 8,192 dynamic (learned) entries in its Bridge Address Table. In addition, it stores up to 200 static or user-defined addresses.

1.5.3 FN10 Filtering

One of the most significant features of the FN10 is its user-configurable filtering capabilities. A filter is an instruction to the FN10 to screen data packets based on the criteria you define. Filtering is useful for gathering statistics, implementing security measures, and improving network performance.

The FN10 allows you to implement two types of filters that are useful for managing and administering networks:

- Bridge Address Table filters, which use the FN10 Bridge Address Table to screen local traffic
- Port filters, which apply filters to or from a specific port segment

See Chapter 5, FN10 **Filters** for instructions on setting up FN10 filters.

1.5.4 FN10 Sample Applications

Just as a six lane highway allows you to travel much faster than a single lane highway, a network backbone creates high-speed connections for your network. In general, a network backbone allows you to distribute access to important network resources such as file or print servers.

Additional FN10 features, such as trunking, Fast Ethernet, and virtual workgroups allow you to optimize bandwidth and design a more efficient flow for your network traffic.

1.5.4.1 FN10 Trunking

The FN10 allows multiple trunk groups with up to eight ports each to be connected between the FN10 and other network devices. This capability provides a scalable dedicated bandwidth of up to 80 Mbps.

For example, local traffic, such as the Manufacturing Department's internal traffic, can be easily handled by a single, 10 Mbps connection. However, when the Manufacturing Department needs access to the corporate database, the traffic could travel over a trunk line, thereby increasing the speed of transmission. Figure 1-5 illustrates the trunking of multiple FN10 ports to increase the bandwidth.

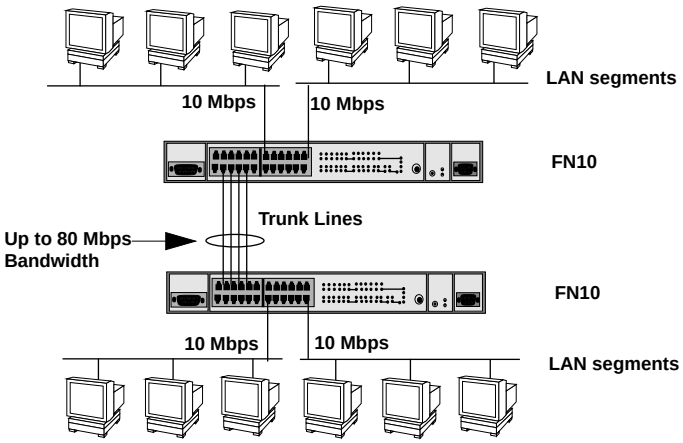


Figure 1-5 FN10 Application #1

Figure 1-6 illustrates how the FN10 can be used in a backbone network configuration.

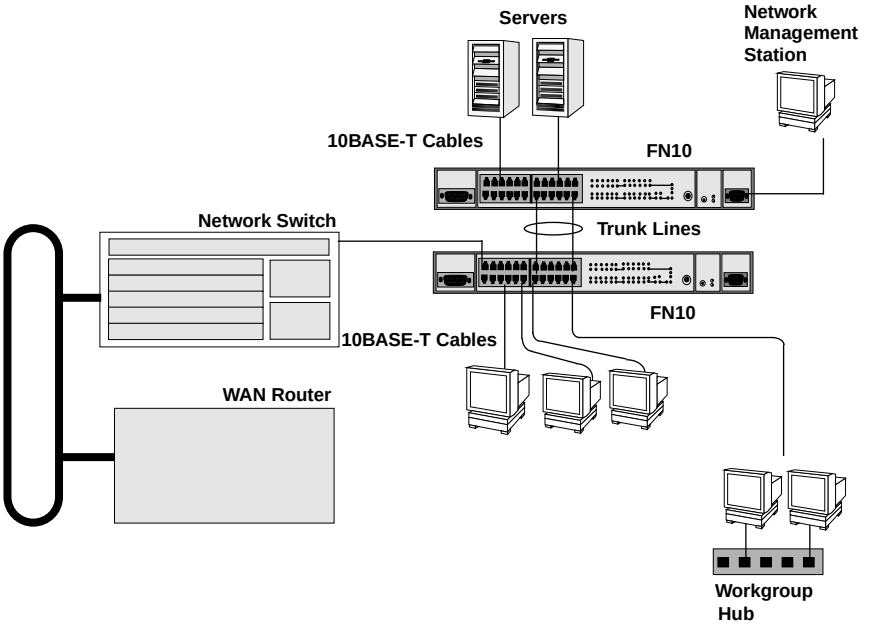


Figure 1-6 FN10 Application #2

1.5.4.2 FN10's Fast Ethernet Option

The FN10, configured with the Fast Ethernet option, has two additional ports that provide a fast Ethernet connection of 100 Mbps. Applying this increased bandwidth to the previous example, the Manufacturing Department's traffic to the corporate database could be transmitted to the corporate database at the 100 Mbps rate.

Figure 1-7 illustrates connecting two FN10 Fast Ethernet ports to increase the bandwidth to 100 Mbps.

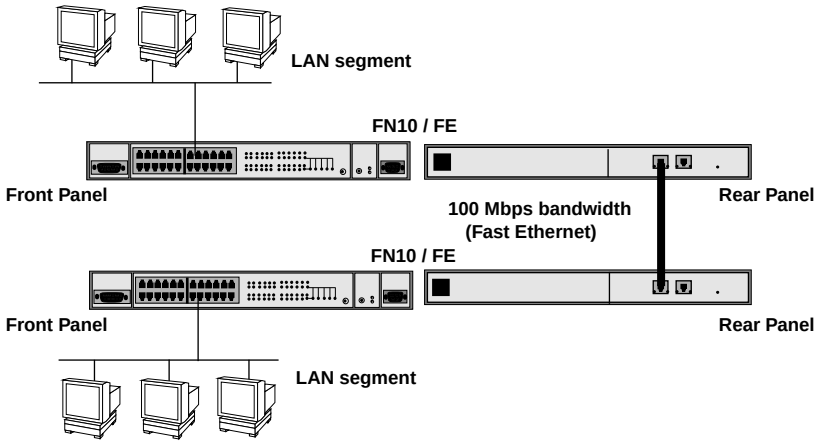


Figure 1-7 FN10 Application #3

Figure 1-8 illustrates how the FN10 can be used in a backbone network configuration using increased bandwidth of the optional Fast Ethernet configuration.

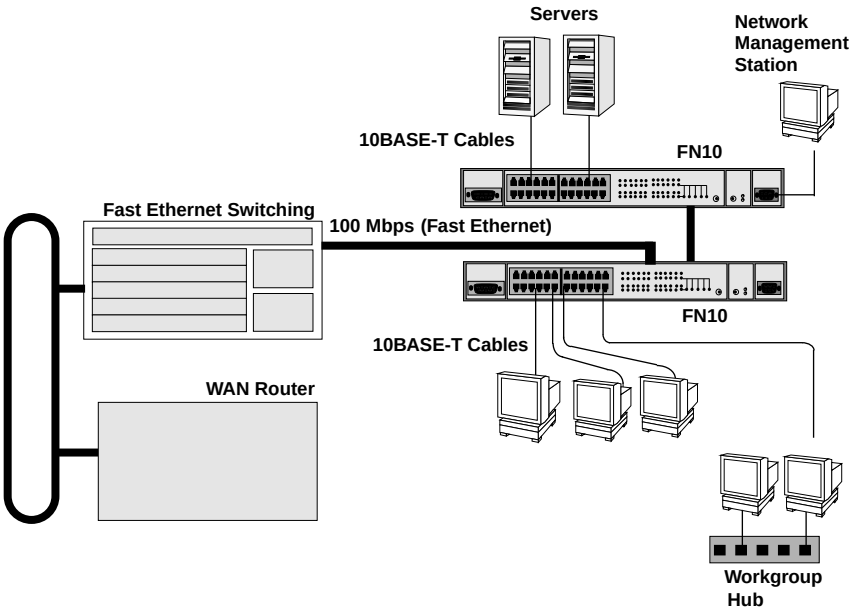


Figure 1-8 FN10 Application #4

1.5.4.3 Virtual Workgroups

The FN10 allows you to define ports for logical groups of associated hosts (virtual workgroups) to provide a more efficient flow of traffic across your Ethernet network.

Virtual workgroups offer you the ability to limit broadcasts to logical domains within the network. Workgroup destinations are recognized by the FN10 and broadcast packets are routed directly to hosts within the workgroup, eliminating the need to perform a general broadcast across each segment of the network to find specific host addresses.

Figure 1-9 shows two Ethernet segments, A and B, that do not include a FN10.

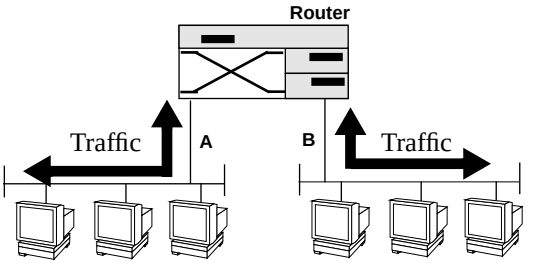


Figure 1-9 Multiple Ethernet Segments Sharing 10 Mbps Bandwidth

Each host on segments A and B is limited to sharing a network bandwidth of 10 Mbps.

Figure 1-10 shows two Ethernet segments that take advantage of the virtual workgroup feature of the FN10 and the increased bandwidth applied to each A and B host.

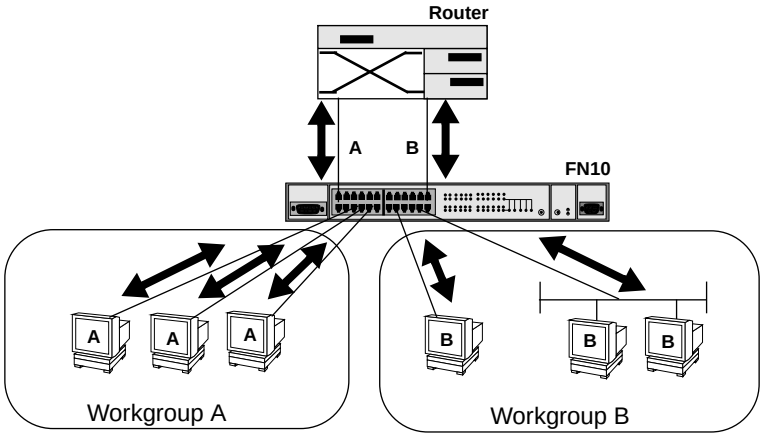


Figure 1-10 Using the FN10 to Create Virtual Workgroups to Help Optimize Bandwidth

A host from workgroup A can limit a broadcast to all hosts within workgroup A or B and prevent the broadcast from going across the network and adding to the amount of contention for the limited 10 Mbps bandwidth.

As illustrated in the previous diagram, virtual workgroups allow you to associate multiple hosts and define a workgroup. In reality, you are assigning workgroup IDs to FN10 ports.

1.6 LOCAL CONSOLE MANAGER

The Local Console Manager (LCM) is a command-line interface built into the FN10 that enables you to monitor, manage, and configure the FN10 through the out-of-band RS232C connection attached to any non-intelligent terminal.

You can also use a Cabletron Systems Network Management System, or a standard SNMP-based Network Management System, to manage the FN10. For a list of available FN10 network management tools, see Section 4-1, **FN10 Management Tools.**

The following sections describe LCM command syntax and the basic LCM commands for logging in, logging out, and getting help.

- LCM commands used for configuring the FN10 are described in Chapter 3, **Configuring Your** FN10.
- LCM commands used for monitoring and managing the FN10 are described in Chapter 4, **Monitoring and Managing Your** FN10.
- LCM commands used for adding and deleting Port filters are described in Chapter 5, FN10 **Filters**.

The FN10 *Local Console Manager (LCM) Commands Reference Card* lists the available LCM commands, including each command's options.

1.6.1 Command Syntax Conventions

The following conventions apply as you use LCM commands:

- Press the **Enter** key to execute a command after you type it in.
- A **port range** is either a single port number, or a list of port numbers separated by commas or hyphens. For example, `3` is port `3`; `3,7` are ports `3` and `7`; `3-5` are ports `3`,`4`, and `5`; and `3-5,7` are ports `3`,`4`,`5`, and 7.
- To quit any command, press the Control-C keys (^C or Ctrl-C).
- You can abbreviate any command where there is no ambiguity; if there is ambiguity, LCM responds with an error message.
- Commands are not case sensitive.
- Any invalid commands or misspellings will receive an error message.
- A previous command can be repeated by typing **`!!`**.
- MAC addresses are displayed in little-endian Ethernet bit order, with each octet separated by a colon. For example:

```
FN10 >address 00:40:27:04:1a:0f
```

- Information that you need to enter with an LCM command is enclosed in square brackets [ ]. For example, you must enter a port number and an IP address to execute the `ipaddr [PORT-NUMBER] [IP ADDRESS]` command:

  ```
  FN10 >ipaddr 6 192.138.217.40
  ```

- Parameters that appear in all capital letters, for example `bridge [PORT-RANGE]`, indicate that you must enter a value for that parameter. If a string of parameters is displayed between braces, for example `[{off|on|noBPDU}]`, you must select one of the displayed options. For example, if you wanted to enable bridging on a port, or a range of ports, you would enter:

  ```
  FN10 >bridge 2-4 on
  ```

- The default values for filtering command field options appear in square brackets [ ], for example:

  ```
  Type:[Entry] (Entry/Exit)>
  ```

1.6.2 Basic LCM Commands

If you are going to manage the FN10 using LCM, you first must connect the FN10 to an ASCII terminal or terminal emulator. See Section 2.3, **Connecting the Local Console Manager**, for instructions.

When you want to use LCM, begin by pressing the **Enter** key several times to get the LCM prompt (`FN10 >`).

1.6.2.1 Help

Displays the menu of available commands. Help can also be displayed by typing a question mark (**?**). The output from the **help** command is displayed below.

```
FN10 > help
                        FN10 Local Console Manager

  help or ?                                      this menu
  status [PORT-RANGE]                            to display unit or port status
  baud [BAUD-RATE]                               to change the console baud rate
  exit or logout                                 to logout
  erase                                          to erase configuration information
  ident                                          to display unit identification
  ipaddr [PORT# IPADDR [MASK]]                   to set or display IP addresses
  addresses display [any] [ADDR [MASK]]          to display learned addresses
  bridge [PORT-RANGE [OPTIONS]]                  to set bridging methods
  trunk [PORT-RANGE [{on | off}]]                to set or display trunking status
  enable [PORT-RANGE [noRIP]]                    to enable a set of ports
  disable [PORT-RANGE]                           to disable a set of ports
  filters {display|modify|add|delete}            to manage port filters
  community                                      to change the password/community name
  sttimer [TIME-VALUE]                           to set or display st age time
  workgroup [NAME [delete|PORT-RANGE [INFO]]]          to set or display workgroups
  speed [PORT-RANGE [{10|100}]]                to set or display Fast Ethernet speed
  reboot {SECONDS | off}                       to reboot the unit after seconds
  arp [display]                                to display arp table information
  route display [IPADDR]                       to display routing table information
  traplog                                      to display the most recent SNMP traps


FN10 >
```

1.6.2.2 Erase

Entering **erase** to erase the current FN10 configuration sets up the IP address on Port 1 to **192.0.2.1** (default) when the FN10 is rebooted.

1.6.2.3 Exit

Logs you out of LCM. (The **exit** command is functionally equivalent to the **logout** command.)

1.6.2.4 Logout

The **logout** command logs you out of LCM. (The **logout** command is functionally equivalent to the **exit** command.)

1.6.2.5 Traplog

Displays the traps messages captured by the FN10. The following is an example of a traplog display:

```
FN10 > traplog
 Trap 16 0:00:00
      The unit has booted.
 Trap 25 0:00:00
      The unit's spanning tree maximum age has changed.
 Trap 26 0:00:00
      The unit's spanning tree hello time has changed.
 Trap 27 0:00:00
      The unit's spanning tree forward delay times has changed.
 Trap 3 0:00:02 port 1
      The current functional state of the port has changed.
   .
   .
   .

 FN10 >
```

CHAPTER 2

UNPACKING AND INSTALLING YOUR FN10

Carefully unpack the FN10 from the shipping carton and inspect it for possible damage. If any damage is evident, contact your supplier. The shipping carton contains the following:

- The FN10 unit
- One AC power cord
- Console Cable kit
- Two rack-mounting brackets with fasteners (for rack-mount installation)
- Four stick-on feet (for desktop installation)
- Documentation – In addition to this manual, the *Fast Network 10 Quick Setup card*, the *Fast Network 10 Local Console Manager (LCM) Commands Reference Card*, the *Fast Network 10 MIB Reference Guide*, and Release Notes are also included.

2.1 FN10 PANELS

The FN10 provides 12 or 24 10BASE-T Ethernet ports, including one Ethernet Attachment Unit Interface (AUI) connection. Each FN10 also includes an RS232C port for out-of-band management, and can be configured with two additional Fast Ethernet (100 Mbps) ports.
Figure 2-1 shows the FN10's front and rear panels. The LEDs and buttons are described in Tables 2-1 and 2-2.

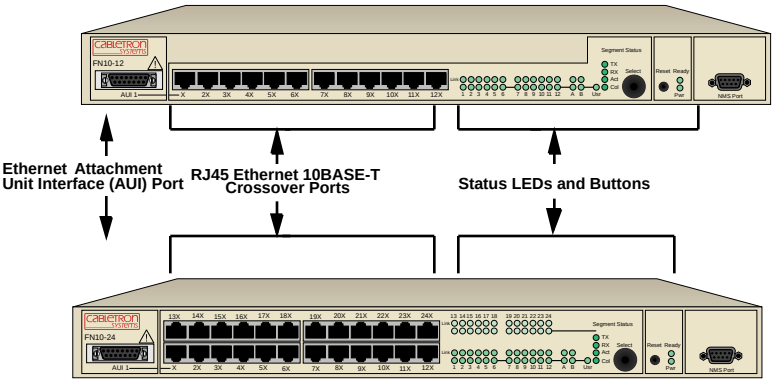


Figure 2-1 FN10 12- and 24-Port Front Panels

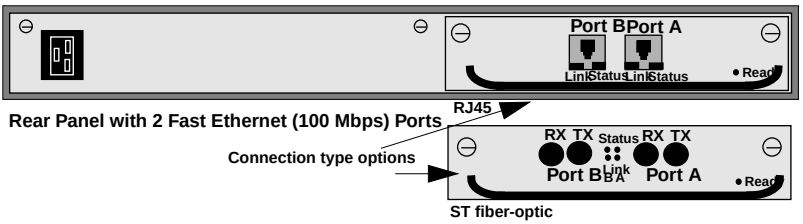


Figure 2-2 FN10 Fast Ethernet (FE) Rear Panel

Table 2-1 Meaning of FN10 LEDs

LED	Meaning
Link (upper level of port LEDs)	On – Indicates the link is good. Off – Indicates there is no link.
Status (lower level of port LEDs)	On/Blinking – Indicates you are monitoring the port for a selected segment status condition. Off – Indicates you are not monitoring the port.
Segment Status TX RX Act Col Usr	 On – Indicates you are monitoring Transmit (TX) activity on all ports. On – Indicates you are monitoring Receive (RX) activity on all ports. On – Indicates you are monitoring Transmit (TX) and Receive (RX) activity on all ports. On – Indicates you are monitoring packet collision on all ports. On – Indicates you are monitoring transmission and receive errors on all ports.
Ready	On – Indicates the FN10 is operational. Blinking – Indicates the FN10 is running power-up diagnostics. Off – Indicates the FN10 is non-operational.
Pwr	On – Indicates the FN10 is receiving power and the voltage is within the acceptable range. Off – Indicates the FN10 is not receiving power.

If the Ready LED continues to blink after power-up diagnostics are complete, it could mean the FN10 is overheating.

Table 2-2 describes the FN10 buttons.

Table 2-2 Description of FN10 Buttons

Button	Function
Select	Cycles through the Segment Status options (TX, RX, Act, Col, and Usr) for all ports. The lower port status LEDs of the ports you are monitoring are activated based on what function you chose with the Select button.
Reset	Restarts the FN10.

2.2 INSTALLING THE FN10

Table-mounting an FN10

If the FN10 is to be table-mounted, make sure you install the four stick-on feet on the bottom of the unit, as shown in Figure 2-3. In addition, make sure the unit is within reach of the network cables to which it will be connected.

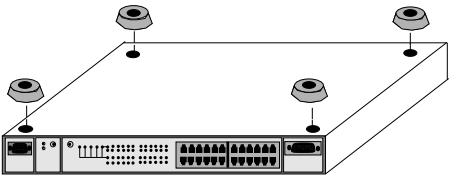


Figure 2-3 Installing the Stick-on Feet

Rack-mounting an FN10

The table below describes some general considerations you should be aware of before mounting a FN10 in a rack assembly.

Table 2-3 General Considerations for Mounting a FN10

Consideration	Discussion
Temperature	Since the temperature within a rack assembly may be higher than the ambient room temperature, make sure the rack-environment temperature is within the Operating Temperature range specified in Appendix A.
Air Flow	Make sure there is at least 2 inches (or more) on both sides of the FN10 to allow for adequate air flow.
Mechanical Loading	Do not place equipment on top of a rack-mounted FN10.
Circuit Overloading	Make sure the power supply circuit to the rack assembly is not overloaded.
Grounding (Earthing)	Rack-mounted equipment should be grounded. In addition to the direct connections to the main power supplies, make sure all the other supply connections are also grounded.

The FN10 can be rack-mounted in a standard 19-inch equipment cabinet. To mount the FN10 in a rack assembly, apply the following steps:

1. Attach the rack-mount brackets to either side of the FN10 chassis.

2. Place the FN10 chassis in the cabinet.
3. Secure the FN10 with the rack-mount fasteners by inserting and securing a fastener through each of the four slots in the rack-mount brackets, as shown in Figure 2-4.

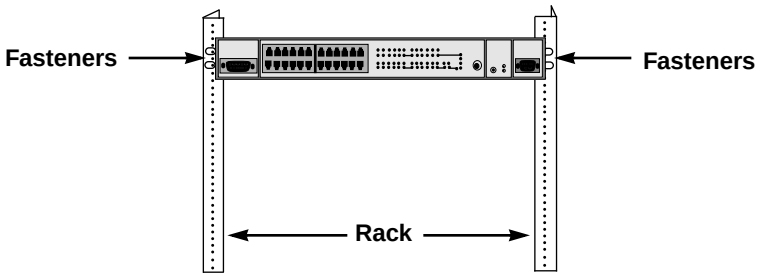


Figure 2-4 Rack-mounting the FN10

4. Once the FN10 is installed, plug the AC power cord into the AC power connector on the rear of the FN10 chassis. Plug the other end of the power cord into a three-prong grounded outlet.

2.2.1 Checking the Power-up Diagnostics Sequence

Before connecting any devices to the FN10, power on the unit and observe the power-up diagnostics sequence to check for proper operation.

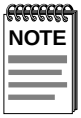
To observe the power-up diagnostics sequence completely, you may want to repeat it. To restart the power-up sequence, turn the power switch OFF, then ON again, or press the reset button on the front panel.

When you power up the FN10, the following occurs:

1. All LEDs, except for the Port Link LEDs, turn on for one second.
2. The Power (Pwr) LED remains on.
3. The Ready LED starts flashing.
4. After several seconds, the Port Link LEDs turn on briefly.

5. After several more seconds, the Ready LED will stay on, indicating that the power-up diagnostics sequence is complete.

   In addition, the Port Link LEDs will turn on for those ports with good links and the Segment Status LEDs will turn on (or flash) when the selected status condition is present.



If a critical component fails diagnostics, the Ready LED will turn off and the FN10 will attempt to reboot. If the Ready LED does not stay on, contact Cabletron Systems Technical Support. Refer to Section 1.2

2.3 CONNECTING THE LOCAL CONSOLE MANAGER

The Local Console Manager (LCM) is a command-line interface for configuring, monitoring, and managing the FN10 through the out-of-band RS232C connection on the front panel.

To connect LCM:

1. Connect your ASCII terminal or terminal emulator to the out-of-band management RS232C port on the front panel of the FN10 using the standard 9-pin serial cable shipped with the unit. (Only three of the nine wires are necessary: Receive Data, Transmit Data, and Ground.)

For your convenience, a male DB-9 to DB-25 converter has been included in the FN10 shipping carton. This converter may come in handy when connecting your ASCII terminal, or terminal emulator.

2. Set the terminal to 9600 baud, 8 data bits, 1 stop bit, and no parity.
3. Press the Enter key several times. If the FN10 is operational, LCM responds with the `FN10 >` prompt.

   LCM is now ready to use.

Refer to Section 1.6, **Local Console Manager** for a general overview of LCM and the command syntax. LCM commands for configuring, monitoring, and managing the FN10 are provided in the chapters dealing with those topics.

See the *FN10 Local Console Manager (LCM) Commands Reference Card* for a list of all LCM commands, including each command's options.

2.4 CONNECTING THE FN10 TO THE NETWORK

Installations vary depending on existing wiring, application objectives, and other considerations. Be sure to have your current network topology map available or contact your network administrator.

The FN10 can be connected via 10BASE-T (or optional Fast Ethernet 100BASE-TX) cable to a punch-down block or patch panel located in a wiring closet. Individual devices are then connected to the FN10 at either the punch-down block or patch panel, usually via unshielded twisted-pair cabling.

For each device you connect to the FN10 through a punch-down block or patch panel, do the following:

1. Connect one end of the 10BASE-T (or optional 100BASE-TX) cable to the device's network interface card.
2. Connect the other end of the 10BASE-T cable to a connector on the punch-down block or patch panel.
3. Connect one end of a second 10BASE-T cable to the connector on the punch-down block or patch panel.
4. Connect the other end of the second 10BASE-T cable to a numbered port on the FN10.

For each device you directly connect to the FN10, do the following:

1. Connect one end of the 10BASE-T (or optional 100 BASE-TX) cable to the device's network interface card.
2. Connect the other end of the 10BASE-T cable to a numbered port on the FN10.

2.4.1 Connecting the AUI Interface

The FN10 includes one Ethernet Attachment Unit Interface (AUI) connector (Port 1). To connect the AUI to a thick coax network, you must use an AUI drop cable and a tap-type transceiver:

1. Attach a tap-type transceiver to the thick coax cable. Refer to the transceiver manufacturer's documentation for installation instructions.
2. Connect one end of the AUI drop cable to the FN10's AUI port and the other end to the tap-type transceiver.

To connect the AUI to an alternate media, such as thin coax, you must use a transceiver connected to the AUI port. Be sure that the transceiver matches the type of Ethernet cable you are using.

The Ethernet Attachment Unit Interface (AUI) Port and Port 1 on the FN10's front panel cannot be used simultaneously. If you connect an RJ45 cable to Port 1 and an AUI cable to the AUI Port, the FN10 automatically uses the RJ45 connection, as long as there is a good link. If there is no link on Port 1, or the link goes down, the FN10 automatically switches to the AUI Port until there is a good link on Port 1.

2.5 ADDING OR REPLACING THE OPTIONAL FAST ETHERNET MODULE

The FN10 is available with an optional Fast Ethernet module to add two additional ports that can be configured for either 10 or 100 Mbps. If you have purchased a FN10/FE, the Fast Ethernet (FE) module is already installed in your FN10.

If you have purchased the FE module separately, or you need to replace an existing FE module, follow the steps below:

1. Disconnect the FN10 from the network and remove the power cord from the rear.
2. Loosen the 2 spring-loaded fastening screws securing the blank backplate and remove the backplate from the FN10. Refer to Figure 2-5.

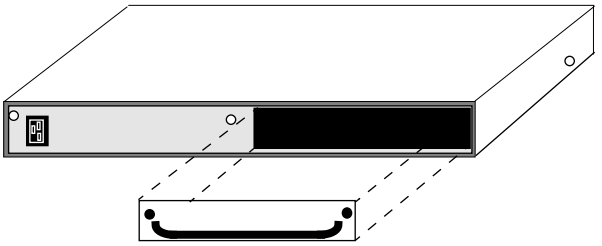
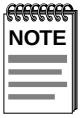


Figure 2-5 Removing the FN10 Backplate



If you are replacing an FE module assembly, slowly pull the module handle away from the FN10 to disconnect the internal connector and slide the assembly out of the FN10.

3. Insert the FE module assembly, making sure the edges of the board fit into the guides that allow the assembly to smoothly glide into place. Refer to Figure 2-6.

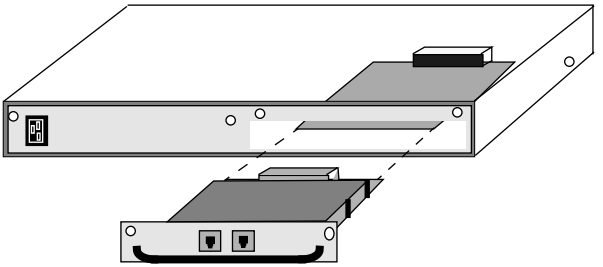


Figure 2-6 Inserting the FE Module Assembly

4. When the FE assembly makes contact with the internal connector, gently press the assembly into the FN10 to allow the connector to snap firmly into place.
5. Tighten the spring-loaded fastening screws to secure the FE module. The physical installation of the FE module assembly is complete.

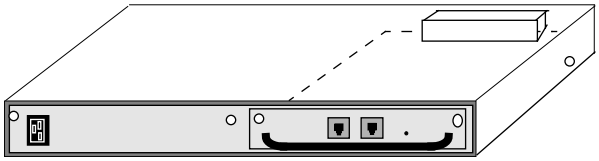


Figure 2-7 Completed FE Module Installation

6. Reconnect the FN10 to the network, plug in the power cord, and power on the unit.
7. Configure the FE module using the LCM command line interface. Refer to Chapter 3, **Configuring Your FN10**.

CHAPTER 3
CONFIGURING YOUR FN10

The FN10 does not require any additional configuration to operate as a standard, transparent switch. However, if you want to use any of the FN10's advanced functions, such as filtering, you must first assign an IP (Internet Protocol) address to any of the ports on the FN10 that you use to communicate with a Simple Network Management Protocol (SNMP) manager.

To initially assign an IP address, you can use the Local Console Manager (LCM). LCM is a command-line interface built into the FN10. It allows you to configure and manage the FN10 through the out-of-band RS232C connection attached to any non-intelligent terminal. (See Section 3.1, **Assigning IP Addresses**.)

Once you have assigned an IP address, you can use any of the following network management tools to configure and manage the FN10:

- Any SNMP-based NMS.

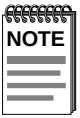
Configuration parameters are stored in an SNMP standard Management Information Base (MIB). All FN10 MIB variables are listed and described in the *Fast Network 10 MIB Reference Guide*.

There are some configuration options that cannot be configured using LCM commands. You may need to modify your configuration using an NMS. See Section 3.11, **Modifying MIB Variables**.

The following sections describe how to configure the FN10 using LCM commands, including:

- Assigning IP addresses
- Enabling and disabling bridging
- Displaying bridging functions
- Enabling and disabling trunking

- Displaying trunking status
- Defining and deleting virtual workgroups
- Assigning a community name



You can use the LCM **erase** command to erase all configuration information on the next system reset.

If you are using a network management tool other than LCM, refer to its accompanying documentation.

3.1 ASSIGNING IP ADDRESSES

IP addresses for each port must be unique. IP addresses are divided into classes based on what portion of the address is network or port information. The address classes are A, B, and C.

- Class A addresses are used in very large networks that support many ports. The first byte identifies the network and the other three bytes identify the node. The first byte of a class A address must be in the range 1-126. The address 100.125.110.10 would identify node 125.110.10 on network 100.
- Class B addresses are used for medium sized networks. The first two bytes identify the network and the last two identify the node. The first byte of a class B address must be in the range 128-191. The address 128.150.50.10 identifies node 50.10 on network 128.150.
- Class C addresses are used for small networks. The first three bytes identify the network and the last byte identifies the port. The first byte of a class C address must be in the range 192-223. The address 192.138.217.10 identifies node 10 on network 192.138.217.

To assign an IP address to a port, at the LCM prompt:

1. Type **`ipaddr <PORT-NUMBER> <IP ADDRESS>`**

   For example, **`ipaddr 6 192.138.217.40`** would set the IP address of Port 6 to 192.138.217.40. LCM responds by displaying the IP address table, as shown under the **`ipaddr`** command.

Entering **`erase`** to erase the current FN10 configuration sets the IP address on Port 1 to **`192.0.2.1`** (default) when the FN10 is rebooted.

3.1.1 Displaying IP Addresses

To display IP addresses, subnet masks, and MAC addresses of all ports on the FN10 you are configuring, at the LCM prompt:

1. Type **ipaddr**

   LCM displays the current IP address table, for example:

```
Port  IP Address          Address Mask        MAC Address
  1   192.138.217.1       255.255.255.0     00:40:27:00:06:1f
  2   0.0.0.0             255.0.0.0         00:40:27:00:06:c3
  3   192.138.217.10      255.255.255.0     00:40:27:00:06:3e
  4   0.0.0.0             255.0.0.0         00:40:27:00:03:7a
  5   0.0.0.0             255.0.0.0         00:40:27:00:05:c7
  6   192.138.217.20      255.255.255.0     00:40:27:00:04:4a
  7   192.138.217.50      255.255.255.0     00:40:27:00:06:9e
  8   192.138.217.30      255.255.255.0     00:40:27:00:04:b4
```

3.1.2 Deleting an IP Address

To delete an IP address, at the LCM prompt:

1. Type **ipaddr <PORT-NUMBER> 0.0.0.0**

   LCM responds by redisplaying the current IP address table.

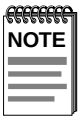
3.1.3 Changing a Subnet Mask

You can optionally set the subnet mask for a port. A subnet mask is a 32-bit address mask used in IP to specify a particular subnet. If the subnet mask is 0.0.0.0, the FN10 will automatically convert the displayed mask to the standard default, based on the port's IP address class. (Class A address masks are 255.0.0.0, Class B address masks are 255.255.0.0, Class C address masks are 255.255.255.0.)

To change the subnet mask, at the LCM prompt:

1. Type **ipaddr <PORT-NUMBER> <IP ADDRESS> <SUBNET MASK>**

   For example, **ipaddr 6 192.138.217.40 255.255.240.0** would set the subnet mask for port 6 to 255.255.240.0. LCM responds by redisplaying the current address table.



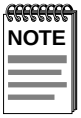
When you change the subnet mask for a port, you must also enter the IP address for that port. Make sure you enter the IP address for the port correctly; whatever you enter becomes the IP address.

3.2 ENABLING BRIDGING

The LCM **bridge** command allows you to set bridging options for a single port or a range of ports. The options include:

- off
- on (the default with BPDU enabled)
- noBPDU

BPDU (Bridge Protocol Data Unit) is a data unit transmitted as part of the IEEE 802.1d Spanning Tree protocol. The exchange of BPDUs allows bridges within a network to logically configure the network as a single spanning tree.



Selecting the **noBPDU** option could make your network inoperable because the FN10 would be unable to detect loops.

Using LCM to enable bridging for a port or port range, at the LCM prompt:

1. Type **bridge [PORT-RANGE [{off|on|noBPDU}]]**

   For example, **bridge 2 on** would enable bridging on port 2.

   LCM responds:

```
Port 2 bridging: Transparent Bridging
```

3.3 DISABLING BRIDGING

To turn off the bridging function for a port or port range, at the LCM prompt:

1. Type **bridge [PORT-RANGE] off**

   For example, **bridge 2 off** would disable bridging on port 2.

   LCM responds:

```
Port 2 bridging: off
```

3.4 DISPLAYING BRIDGING FUNCTIONS

To display the bridging functions that are enabled for all ports, at the LCM prompt:

1. Type **bridge**

   LCM responds with a list of all ports and the bridging function that is enabled. For example, typing **bridge** would display the bridging status for all ports.

```
Usage: bridge [PORT-RANGE [{off|on|noBPDU{]]
  Port 1 bridging: Transparent Bridging
  Port 2 bridging: Transparent Bridging
  Port 3 bridging: Transparent Bridging
  Port 4 bridging: Transparent Bridging
                    .
                    .
                    .
  Port 24 bridging: off
```

   You could also type **bridge [PORT-RANGE]** to look at a specific range of ports. For example **bridge 2-4** would display bridging functions for ports 2, 3, and 4.

3.5 ENABLING TRUNKING

If your network configuration requires you to connect two or more FN10s together, but the applications you are running over the network require more than 10 Mbps of bandwidth per connection, you can use the built-in trunking feature to increase bandwidth up to 80 Mbps, without installing additional hardware on your network.

Trunking is a Cabletron Systems proprietary extension to the 802.1D Spanning Tree algorithm. It enables you to use multiple 10BASE-T Ethernet segments to connect FN10s together, while maintaining first-in, first-out ordering of Ethernet packets. In addition, if any of the Ethernet segments configured for trunking become inoperable, those Ethernet segments are automatically bypassed.

Figure 3-1 shows two FN10s connected by four 10BASE-T crossover cables. You can connect up to eight ports for sharing the traffic load. Any additional connected ports will become *standby* ports. The connections must be point-to-point. That is, there cannot be any other devices on the Ethernet segments.

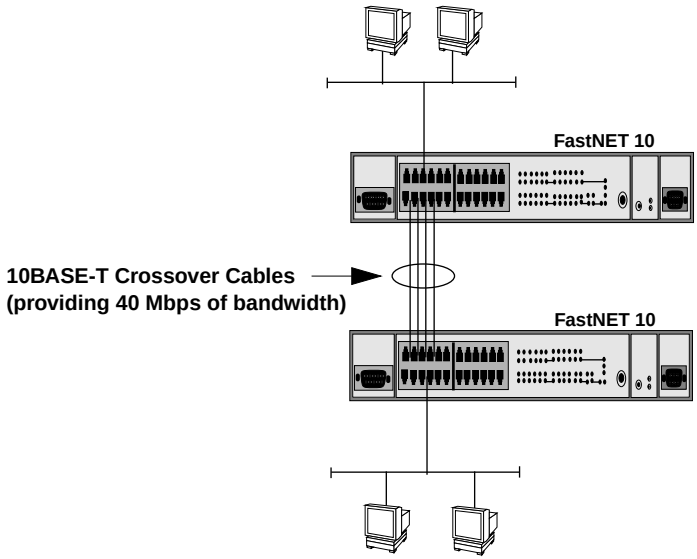


Figure 3-1 Trunk Connections

NOTE

In some wiring closets, it may be easier to connect two FN10s via an Ethernet concentrator. However, you must make sure that there are no other devices connected to the Ethernet concentrator.

Trunk Groups

Each set of connections between two FN10s is called a *Trunk Group*. You can create several Trunk Groups to interconnect your FN10s. Each FN10 can have up to four Trunk Groups.

For example, if you have three FN10s (A, B, and C), as shown in Figure 3-2, you could connect them using a single Ethernet segment. However, that would limit the interconnection to 10 Mbps. To solve this problem, you could connect **A to B** with one Trunk Group, and connect **B to C** with a second Trunk Group.

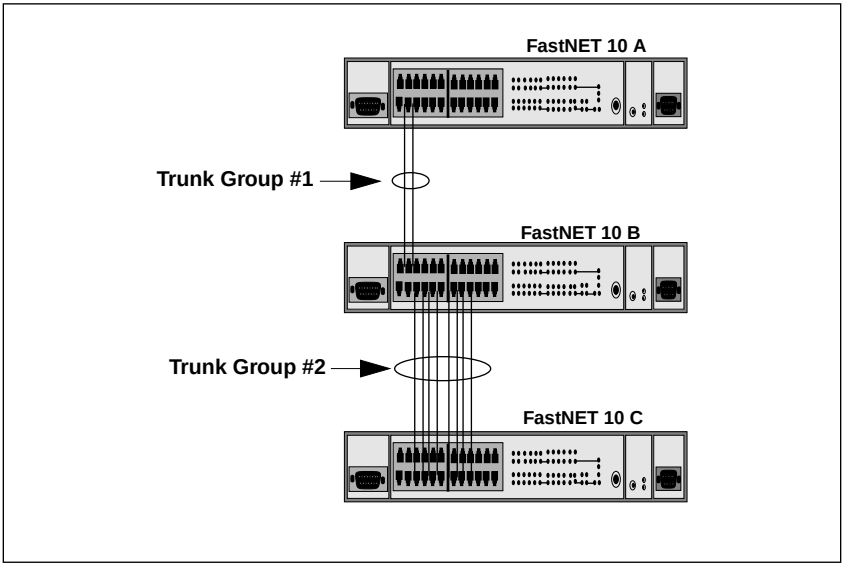


Figure 3-2 Trunk Groups

To enable trunking for the example shown, you would:

1. Connect the desired ports of the FN10s together using 10BASE-T crossover cables.

   If FN10 A is handling only a small number of users, the **A to B** Trunk Group could have just two ports per FN10. If FN10 B and C are expected to interconnect many users, you could use up to eight ports in the **B to C** Trunk Group.

2. Using LCM, turn on trunking for the connected ports on each FN10.

   For FN10 A, at the LCM prompt:

   a. Type **`trunk 2,3 on`**

   For FN10 B, at the LCM prompt:

   b. Type **`trunk 3-10,14-15 on`**

   For FN10 C, at the LCM prompt:

   c. Type **`trunk 3-10 on`**

   Each FN10 automatically determines which ports are part of which Trunk Group. After Trunk Group configuration, the FN10s complete the standard 802.1D Spanning Tree state changes, treating each Trunk Group as a single 802.1D Spanning Tree port.

   802.1D Spanning Tree takes about thirty seconds to resolve which FN10 ports are to become forwarding ports. As ports within a Trunk Group become forwarding ports, traffic within the Trunk Group is momentarily halted to guarantee the first-in, first-out ordering of the Ethernet packets.

The FN10-to-FN10 connections must be point-to-point. There cannot be any other devices on those Ethernets. The ports used for trunking can be in any order. However, both ends of the FN10-to-FN10 connections must have trunking turned on for the ports that are being used for the connections.

3.6 DISABLING TRUNKING

To turn off trunking, at the LCM prompt:

1. Type **trunk <PORT-RANGE> off**

   For example, **trunk 2-4 off**

3.7 DISPLAYING TRUNKING STATUS

To check the status of your current trunking configuration, at the LCM prompt:

1. Type **trunk <PORT-RANGE>**

The display could look like the following:

```
FN10 > trunk 2-4

Port 2 trunking joined to Bridge MAC Addr 00:40:27:00:06:1f IP Addr 192.138.217.1
Port 3 trunking joined to Bridge MAC Addr 00:40:27:00:06:c3 IP Addr 192.138.200.2
Port 4 trunking joined to Bridge MAC Addr 00:50:36:00:07:4a IP Addr 192.140.250.7
```

The following conditions can be displayed:

- Closed (or Oneway) — Trunking is enabled, and the Trunking Protocol is attempting to establish a trunk connection.
- Heldown — Trunking is enabled, but the trunk connection was rejected. After a short time-out period, another attempt is automatically initiated to establish a good trunk connection.
- Joined — Trunking is enabled, and the Trunking Protocol has established a good trunk connection.
- Off — Trunking is not enabled.
- Perturbed — Trunking is enabled, and a good trunk connection has been established. However, the forwarding of data packets is temporarily suspended to allow for a change in the membership of the Trunk Group.

To check the status for ports configured for trunking, at the LCM prompt:

1. Type **status <PORT-RANGE>**

The display could look like the following:

```
FN10 > status 1

          Port 1 Status

 Bridging:             Transparent Bridging
 Enabled/Disabled:     Enabled, Rip listening
 Spanning Tree:        Forwarding
 Trunking State:       Off
 Pkts Transmitted:     1693
 Pkts Received:        0
 Carrier Losses:       1693
 Total Collisions:     0
 Excess Collisions:    0
 RX Missed Pkts:       0
 RX Runt Pkts:         0
 RX FCS/Align Errs:    0
 Internal TX Errs:     0

 Type <CR> to display port 2 status...>
```

The following conditions can be displayed:

- Broken — Trunking is enabled, but the port in non-operational.
- Closed (or Oneway) — Trunking is enabled, and the Trunking Protocol is attempting to establish a trunk connection.
- Heldown — Trunking is enabled, but the trunk connection was rejected. After a short time-out period, another attempt is automatically initiated to establish a good trunk connection.
- Joined — Trunking is enabled, and the Trunking Protocol has established a good trunk connection.
- Off — Trunking is not enabled.
- Perturbed — Trunking is enabled, and a good trunk connection has been established. However, the forwarding of data packets is temporarily suspended to allow for a change in the membership of the Trunk Group.

3.8 DEFINING AND DELETING WORKGROUPS

The FN10 allows you to define logical groups of associated hosts (virtual workgroups) to provide a more efficient flow of traffic across your Ethernet network.

Virtual workgroups offer you the ability to limit broadcasts to logical domains within the network. Workgroup destinations are recognized by the FN10 and packets are routed directly to hosts within the workgroup, eliminating the need to perform a general broadcast across each segment of the network to find specific host addresses.

Figure 3-3 shows a FN10 that has been programmed to identify workgroups A and B. Workgroup A uses ports 3 through 5, and workgroup B uses ports 7 and 11. Port 16 connects a segment that contains both workgroup A and workgroup B hosts.

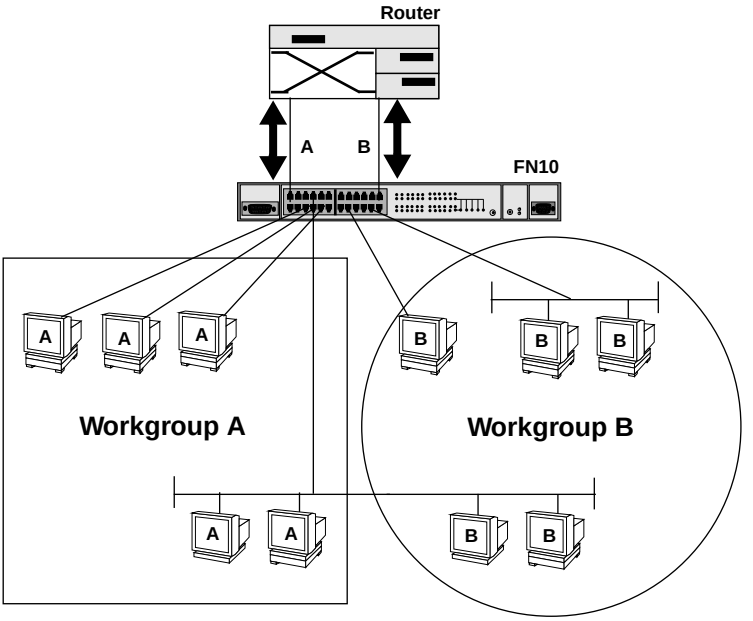


Figure 3-3 Defining Virtual Workgroups

The LCM commands used to create the previous configuration are as follows:

1. To create workgroup A on ports 3, 4, 5, 13, and 16:

   ```
   FN10 > workgroup A 3-5,13,16
   ```

   LCM responds with the following display:

   ```
   Name: a
   Ports: 3, 4, 5, 13, 16
   Info: all
   ```

2. To create workgroup B on ports 7, 11, 16, and 24:

   ```
   FN10 > workgroup B 7,11,16,24
   ```

   LCM responds with the following display:

   ```
   Name: b
   Ports: 7, 11, 16, 24
   Info: all
   ```

Port 16 has been assigned to a segment that includes hosts that belong to workgroup A and workgroup B. Port 13 connects workgroup A to the router and port 24 connects workgroup B to the router.

In the above steps, both command lines did not specify a specific classification of workgroup and have defaulted to the *all* category that allows broadcasts of any protocol. To specify a specific IP network you would need to add the IP network ID.

The following LCM commands re-define the previous example as workgroups with an IP network classification:

1. To create workgroup A:

   ```
   FN10 > workgroup A 3-5,13,16 ip 198.113.120.0
   ```

   LCM responds with the following display:

   ```
   Name: a
   Ports: 3, 4, 5, 13, 16
   Info: IP 198.113.120.0 255.255.255.0
   ```

2. To create workgroup B:

```
FN10 > workgroup B 7,11,16,24 ip 198.113.121.0
```

LCM responds with the following display:

```
Name: b
Ports: 7, 11, 16, 24
Info: IP 198.113.121.0 255.255.255.0
```

In both cases, a specific NETMASK value was omitted and LCM assumed the standard IP address class mask.

As illustrated in the previous example, virtual workgroups allow you to associate multiple hosts, define a workgroup, or delete a workgroup. In reality, you are assigning workgroup IDs to FN10 ports.

Use the LCM command, *workgroup*, to create, modify, and delete virtual workgroups. The full syntax of the command is as follows:

workgroup [NAME [{delete | PORT-RANGE [INFO]}]]

The options for **INFO** include:

- ip IP-ADDRESS [NETMASK] - indicates an IP network and if NETMASK is omitted, the standard IP class mask is assumed.
- ipx [IPX-NETWORK] - indicates an IPX network and if IPX-NETWORK is omitted all IPX numbers will be assumed (this is referred to as the default workgroup).
- all - allows any network protocol and is the default setting for the workgroup command.

To display all of the workgroups defined by the FN10, at the LCM prompt:

1. Type **`workgroup`**

To display information about a specific workgroup, at the LCM prompt:

1. Type **`workgroup NAME`**

To create or modify a workgroup, at the LCM prompt:

1. Type **`workgroup NAME PORT-RANGE INFO`**

To delete a workgroup, at the LCM prompt:

1. Type **`workgroup NAME delete`**

To create or modify the port list for a specific workgroup, at the LCM prompt:

1. Type **`workgroup NAME PORT-RANGE`**

To modify the network classification of a specific workgroup, at the LCM prompt:

1. Type **`workgroup NAME INFO`**

3.9 ASSIGNING A COMMUNITY NAME

A community name is similar to a password. You use the same steps to assign a new community name or to change an existing community name. This sets the MIB variable `sxadminAnyPass`. You can then enter a community name to perform any SNMP *sets*. The default password is an empty string that allows you to enter your community name.

To assign a community name, at the LCM prompt:

1. Type **`community`**
2. Enter the old community name.

   If one has not been assigned, you do not need to enter anything. LCM prompts you for the new community name.
3. Enter the new community name.

   LCM prompts you to verify the new community name by retyping it.
4. Retype the new community name.

3.10 CONFIGURING MULTICAST STORM PROTECTION

The FN10 provides automatic protection against multicast storms. Multicast storms are excessive broadcasts to all ports, typically caused by a malfunctioning device. They can result in severe network performance problems, including causing the network to crash.

To protect against multicast storms, you must define an acceptable rate for multicast traffic across a port. In many ways, this feature is similar to filtering, however, multicast storm protection does not involve the use of filters.

Each FN10 port can be individually configured for automatic multicast storm protection. You define what level of multicasts the FN10 will recognize as a multicast storm by specifying the number of multicast packets that can be transmitted within a given time period.

LCM does not allow you configure for multicast storm protection. You must use RCM or an SNMP-based NMS. See the *RCM Reference Guide* or the documentation that came with your NMS for configuration instructions.

For example, if you configure FN10 to transmit onto Port 3 no more than five multicasts per 60 seconds, any multicasts destined for Port 3 are discarded after the first five multicasts. After 60 seconds have elapsed, another five multicasts to Port 3 will be allowed. This maintains an effective maximum rate of five multicast packets per minute.

The two Management Information Base (MIB) variables for configuring multicast storm protection are:

- `sxifTxStormCnt` – specifies the maximum number of multicasts that can be broadcast within the given time.
- `sxiTxStormTime` – specifies the period of time that the maximum number of multicasts can be broadcasted.

Refer to the *Fast Network 10 MIB Reference Guide* for a complete listing and description of MIB variables.

3.11 MODIFYING MIB VARIABLES

Specific instructions for controlling FN10 operations, modifying parameters, and so on, depend on the NMS you are using. This manual provides instructions for using LCM commands. However, LCM commands do not exist for all configuration options. You may need to modify your configuration using an NMS.

This section provides several common MIB variables you may want to change. Refer to the *Fast Network 10 MIB Reference Guide* for a complete listing and description of MIB variables.

Each variable is first described in words, and is then identified in MIB form, for example, `sxadminGetPass - {sxadmin 3}`. The Display String line shows the range of values that can be used for the given parameter. In each case, the DisplayString is a string of ASCII characters.

3.11.1 System Contact

The system contact parameter identifies the contact person who is responsible for operating the FastNET 10. Typically, this parameter includes the person's name, company or division name, and telephone number.

```
    sysContact - {system 4}
DisplayString (SIZE (0..255))
```

3.11.2 System Name

The system name is a name assigned to the FN10 by the network administrator. By convention, the system name is the fully qualified domain name. (This name then becomes the LCM prompt.)

```
    sysName - {system 5}
DisplayString (SIZE (0..255))
```

3.11.3 System Location

The system location identifies the physical location of the FN10.

```
    sysLocation - {system 6}
DisplayString (SIZE (0..255))
```

3.11.4 Authentication Password

The set password and get password variables (from the SMC proprietary MIB), must be initialized with the correct authentication passwords.

All requests from any SNMP manager contain a community name field. For set requests, the community name must match the set password; otherwise, the request will be rejected by the FN10. For get requests, the community name must match either the set password or the get password.

Set Password

The set password variable (`sxadminAnyPass`) must be set to the value of the community name used by the SNMP manager for performing either set or get operations. A zero length password means that any community name is acceptable.

```
        sxadminAnyPass - {sxadmin 2}
    DisplayString (SIZE (0..24))
```

Get Password

The get password variable (`sxadminGetPass`) must be set to the value of the community name used by the SNMP manager for performing get operations. A zero length password means that any community name is acceptable.

```
        sxadminGetPass - {sxadmin 3}
    DisplayString (SIZE (0..24))
```

3.11.5 Aging Parameter

Dynamic (learned) addresses are automatically deleted from the FN10 Bridge Address Table after a certain length of time. The aging time default is five minutes, as set by the IEEE 802.1d standard. However, you can change the aging parameter using the MIB variable `dot1dTpAgingTime`.

The FN10 continually compares the actual age of each dynamic address against the age specified by the `dot1dTpAgingTime` parameter, and deletes any addresses that are older than the age specified (or older than five minutes if you are using the default). Typically, there is no need to set the aging time to a very small number because the FN10 Bridge Address Table supports 8,192 addresses.

Static addresses (those added by the user) are not aged.

CHAPTER 4

MONITORING AND MANAGING YOUR FN10

Monitoring the FN10 consists of collecting and analyzing statistics and system status information. Additional statistics gathered by the FN10 are the result of user-configurable filters. See Chapter 5, **FN10 Filters**, for information on setting up FN10 filters.

You can use the Select button on the front panel of the FN10 to monitor segment status on any of the Ethernet ports. Refer to Section 2.1 for a description of the segment status options.

Basic management of the FN10 consists of disabling or enabling Ethernet ports, changing subnet masks, setting the community name for the FN10, and changing the baud rate for your Local Console Manager (LCM) connection.

4.1 FN10 MANAGEMENT TOOLS

LCM is a command-line interface built into the FN10 that enables you to monitor and manage the FN10 through the out-of-band RS232C connection attached to any non-intelligent terminal. You can also use one of the following Cabletron Systems Network Management Stations (NMSs), or a standard SNMP-based NMS to manage the FN10:

- Any SNMP-based NMS.

4.2 FN10 STATISTICS

The FN10 gathers statistics that can help you build a comprehensive profile of the network traffic flow between each Local Area Network (LAN) you are connecting, as well as the network traffic flow to and from each Ethernet port on the FN10.

FN10 statistics are divided into five groups:

- System statistics
- Ethernet port statistics

- MAC statistics
- Traffic analysis statistics
- SNMP statistics

You can use this information to analyze your overall network performance and to make configuration changes as necessary. For example, Ethernet port statistics can help you identify network devices that require high bandwidth, and therefore should be connected through a dedicated, rather than a shared, network connection. In addition, Ethernet port statistics can help you identify a network device that is the source of numerous multicast packets due to a possible malfunction.

4.2.1 Pseudo Filters

You can configure pseudo-filters to optimize your network design. Pseudo-filters generate statistics as if a filter had actually been applied without actually invoking the filter or impacting the network. See Chapter 5, **Fast Network 10 Filters** for information on setting up FN10 filters.

4.2.2 Gathering Statistics

For purposes of network management, managed objects, such as the FN10, must be identified. Creation of a managed object is achieved by placing its identifier, and a set of management information appropriate to its class, in the Management Information Database (MIB).

Using the MIB variables, you can obtain a detailed analysis of your network by combining statistics for each source network, destination network, and source and destination port. The *Fast Network 10 MIB Reference Guide* contains the SNMP MIB variables you need to monitor and manage the FN10.

4.2.3 System Statistics

For each FN10, the following system statistics are available:

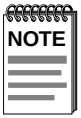
- The number of seconds since the FN10 was last reset.
- The number of spanning tree topology changes that have occurred since the FN10 was last reset.
- The time since a topology change was last initiated.
- The physical location of the FN10.
- The name and address of the contact person for the FN10.
- The name of the FN10.
- The number of times an address was not added to the FN10 Bridging Address Table because the table was full.
- The current number of dynamic (learned) addresses.
- The current number of static addresses.

- The number of times each filter was successfully invoked, and the source address of the packet for the last successful invocation of each of the combination filters.

To check FN10 system status using LCM, see Section 4.3.

4.2.4 Ethernet Port Statistics

For each Ethernet port connection on the FN10, the following statistics are available. They can help you analyze both network activity and utilization, and in some cases, indicate faulty equipment or cabling.



All statistics counters are cleared when the FN10 is reset or when Ethernet ports are re-enabled.

- The number of packets received from the port.

  The packets are broken down into the following categories by type of destination address:

  - Known individual destination address
  - Unknown individual destination address
  - Multicast address (other than broadcast)
  - Broadcast address
  - Individual node management packets
  - Multicast node management packets (other than broadcast)
  - Broadcast node management packets

For each of the above categories, statistics on whether a packet was forwarded or filtered are available. In addition, if a packet was filtered, the following conditions are recorded:

- If the packet is local traffic
- If the port is not in the Spanning Tree Forwarding state
- If there is a source address or entry port restriction
- If there is a destination address or exit port restriction

- The number of bytes in the received packets.
- The number of bytes in the packets that were filtered.
- The number of bytes in the packets that were forwarded.
- The total number of packets transmitted to the LAN.

  The packets are broken down into the following categories by type of destination address:

  - Known individual destination address
  - Unknown individual destination address
  - Multicast address (other than broadcast)
  - Broadcast address
  - Individual node management packets
  - Multicast node management packets (other than broadcast)
  - Broadcast node management packets
- The number of bytes in the transmitted packets.
- The number of packets not transmitted to the LAN.

  The packets are broken down into the following categories:

  - Not sent due to congestion
  - Not sent due to multicast storm protection
- The number of received Frame Check Sequence (FCS) errors detected.
- The number of missed packets due to receive queue overflows.

- The number of received packets with frame alignment errors.
- The number of packet transmissions that were initially deferred due to the media being busy.
- The number of packets not transmitted due to excessive collisions.
- The number of packets transmitted with one collision.
- The number of packets transmitted with multiple collisions.
- The number of RX and TX collisions.

4.2.5 MAC Statistics

Media Access Control (MAC) statistics are available for each MAC address stored in the FN10 Bridging Address Table. They can help you determine how many packets are being sent and received by a specific device on the network.

- The number of seconds since receiving a packet from the device with a specific address.
- The number of seconds since transmitting a packet to the device with a specific address.
- The number of packets received from the device with a specific address.
- The number of packets transmitted to the device with a specific address.
- The number of bytes received from the device with a specific address.
- The number of bytes transmitted to the device with a specific address.
- The number of multicast packets received from the device with a specific address.
- Number of packets forwarded from the device with a specific address.

The receive statistics for the entries in the FN10 Bridging Address Table are only updated when packets are received on Ethernet ports that are in Spanning Tree Forwarding or Learning state, and if Learning has been enabled on the Ethernet port.

4.2.6 Traffic Analysis Statistics

You can configure the FN10 to collect statistics on traffic between active Ethernet ports, for example:

- Number of packets sent from Station A to Station B.

  Configure pseudo source-port filter with Station A's address as source address match and Station B's address as destination address match.

- Number of IP packets sent from Station A to Station B.

  Configure pseudo source-filter with Station A's address as source address match and Stations B's address as destination address match and Frame Type set to IP.

- Number of packets sent from Station A to Segment B.

  Configure pseudo destination filter on port B with Station A's address as source address match.

- Number of packets sent from Segment A to Station B.

  Configure pseudo source filter on port A with Station B's address as destination address match.

Refer to Chapter 5, **FN10 Filters**, for instructions on setting up FN10 pseudo filters.

4.2.7 SNMP Statistics

The following statistics relate specifically to SNMP. The Management Information Base (MIB) variable that collects the statistics is provided in square brackets.

- The number of SNMP PDUs received by the FN10. [`snmpInPkts`]
- The number of SNMP PDUs created by the FN10. [`snmpOutPkts`]
- The number of SNMP PDUs received by the FN10 which had an unsupported SNMP version. [`snmpInBadVersions`]
- The number of SNMP PDUs received by the FN10 which had an unrecognized SNMP community name. [`snmpInBadCommunityNames`]
- The number of SNMP PDUs received by the FN10 which had an authentication failure. [`snmpInBadCommunityUses`]

- The number of SNMP PDUs received by the FN10 which had an ASN.1 parsing error while being decoded by the FN10. [snmpInASNParseErrs]
- The total number of MIB objects which have been successfully retrieved by the FN10 as a result of SNMP GetRequest or GetNext PDUs. [snmpInTotalReqVars]
- The total number of MIB objects which have been successfully altered by the FN10 as a result of SNMP SetRequest PDUs. [snmpInTotalSetVars]
- The total number of SNMP GetRequest PDUs received by the FN10, which have been processed with no errors. [snmpInGetRequests]
- The total number of SNMP GetNext PDUs received by the FN10, which have been processed with no errors. [snmpInGetNexts]
- The total number of SNMP SetRequest PDUs received by the FN10, which have been processed with no errors. [snmpInSetRequests]
- The total number of SNMP PDUs created by the FN10, with a value of tooBig in the PDU's ErrorStatus. [snmpOutTooBigs]
- The total number of SNMP PDUs created by the FN10, with a value of noSuchName in the PDU's ErrorStatus. [snmpOutNoSuchNames]
- The total number of SNMP PDUs created by the FN10, with a value of badValue in the PDU's ErrorStatus. [snmpOutBadValues]
- The total number of SNMP PDUs created by the FN10, with a value of genErr in the PDU's ErrorStatus. [snmpOutGenErrs]
- The total number of SNMP GetResponse PDUs created by the FN10. [snmpOutGetResponses]
- The total number of SNMP Trap PDUs created by the FN10. [snmpOutTraps]

4.3 USING LCM TO CHECK FN10 STATUS

The LCM commands that enable you to quickly check on the status of the FN10 include:

- Status

- Address display
- Ipaddr
- Ident

These LCM commands are described in the sections that follow.

4.3.1 Displaying Status

The **status** command displays the status of the FN10 and automatically pages through the status of all of the Ethernet ports, pausing at each screen of information.

You can also use the **status** command to display status for individual Ethernet ports by typing **status** and specifying a port number.

At the LCM prompt:

1. Type **status**

   LCM displays the following type of information.

```
Software Currently Running: TigerSwitch software, Tue 08/23/94 15:03:09
Next Bootstrap (1st bank): TigerSwitch software Tue 08/23/94 15:03:09
Power-up test failures: none
Current unit temperature is normal.
System Up Time: 2:25:57
Current Number of Learned Addresses: 133
Number of Defined Filters: 0
CPU utilization is light.

Port     RX Packets     TX Packets     Collisions    Erred Packets
  1              0           1676              0             1676
  2           6978              8              0                0
  3              0              0              0                0
  4              0              0              0                0
  .              .              .              .                .
  .              .              .              .                .
  .              .              .              .                .
 24              0              0              0                0

Type <CR> to display port 1 status...>
```

If you do not want to view the status of each Ethernet port, use the Ctrl-C keys to return to the LCM prompt.

```
          Port 1 Status

Bridging:             Transparent Bridging
Enabled/Disabled:     Enabled, Rip listening
Spanning Tree:        Forwarding
Trunking State:       Off
Pkts Transmitted:     1693
Pkts Received:        0
Carrier Losses:       1693
Total Collisions:     0
Excess Collisions:    0
RX Missed Pkts:       0
RX Runt Pkts:         0
RX FCS/Align Errs:    0
Internal TX Errs:     0

Type <CR> to display port 2 status...>
```

If you do not want to view the status of port 2, use the Ctrl-C keys to return to the LCM prompt.

You can view the status for multiple of ports by typing **`status`** and indicating the range of port numbers, for example **`status 2-6`**.

4.3.2 Displaying MAC Addresses

The **`addresses display`** command displays all MAC addresses in the FN10 Bridge Address Table. The display includes:

- The MAC address
- Type of address, including:
  - Dynamic (learned)
  - Ethernet port (for the MAC address of an Ethernet port)
  - Static (for an address that was added by an NMS)
  - BPDU (the MAC address to which all BPDUs are directed)
  - Reserved (the address reserved by 802.1d, but not yet assigned)
  - All LANs (the addresses reserved by 802.1d for network management)
- Port number
- Age (in seconds since a packet was last received from that address)
- Number of packets received from that address
- Number of packets forwarded to that address

The display automatically pauses with each screen of information. Addresses are displayed in random order; for example, address 02:00:00:00:00:00 may appear after address 04:00:00:00:00:00.

The age will be the most recent of the following:

- Time since a packet was last received from that address
- Time since that address was created (e.g., a static address created by an NMS)

To display all MAC addresses, at the LCM prompt:

1. Type **addresses display any**

   LCM responds with a list of all MAC addresses, their associated ports, the type, age, and number of frames from and to that address.

```
Address            Type     Port  Age(secs)  Frames-From   Frames-To
08:00:20:02:3a:44  Learned    3          26            1           0
00:40:27:03:b7:21  Static     **          5        17110         195
 Enter <CR> to continue, Ctrl-C to exit:
```

If you do not specify **any**, only the learned static and other addresses are displayed.

To display a specific address, at the LCM prompt:

1. Type **addresses display <MAC-ADDRESS>**

   For example, if you typed, **addresses display 02:04:06:03:2a:43**, LCM would display the following information:

```
Address            Type     Port   Age(secs)   Frames-From    Frames-To
02:04:06:03:2a:43  Learned     5           21          1181           73
```

You can display a range of addresses by using a net mask. This is helpful when determining the status associated with stations containing the same make of Ethernet network interface cards. At the LCM prompt:

1. Type **addresses display <MAC-ADDRESS> <NET-MASK>**

   For example, to see all addresses that begin with 02:04:06, you would enter:

```
addresses display 02:04:06:00:00:00 ff:ff:ff:00:00:00
```

LCM would display:

```
Address              Type     Port   Age(secs)    Frames-From    Frames-To
02:04:06:03:2a:43   Learned     5          21           1181           73
02:04:06:00:2a:67   Learned     4           1           3421            0
02:04:06:a3:70:2b   Learned     6           0          15339          235
Enter <CR> to continue, Ctrl-C to exit:
```

LCM allows you to display MAC addresses in two formats:

- Little-endian (default)

  Little-endian is a method of storing or transmitting data in which the least significant bit of each byte is presented first. This is used in Ethernet networks.

- Big-endian

  Big-endian is a method of storing or transmitting data in which the most significant bit of each byte is presented first. Use the **`big`** option to display MAC addresses in big-endian format.

  Big-endian format separates the bytes with spaces rather than colons. You can also enter MAC addresses in big-endian format by using spaces rather than colons. This option is helpful if your network includes Token Ring or FDDI along with Ethernet.

The **`ipaddr`** command displays the IP addresses, subnet masks, and MAC addresses of all FN10 ports. At the LCM prompt:

1. Type **`ipaddr`**

   LCM displays the current IP address table, for example.

```
 Port    IP Address            Address Mask            MAC Address
   1     192.138.217.1         255.255.255.0        00:40:27:00:06:1f
   2     0.0.0.0               255.0.0.0            00:40:27:00:06:c3
   3     192.138.217.10        255.255.255.0        00:40:27:00:06:3e
   4     0.0.0.0               255.0.0.0            00:40:27:00:03:7a
   5     0.0.0.0               255.0.0.0            00:40:27:00:05:c7
   6     192.138.217.20        255.255.255.0        00:40:27:00:04:4a
   7     192.138.217.50        255.255.255.0        00:40:27:00:06:9e
   8     192.138.217.30        255.255.255.0        00:40:27:00:04:b4
```

4.3.3 Displaying Manufacturing Information

The **ident** command identifies FN10 manufacturing information, including the part number and any power-up test codes and diagnostic data. To display the manufacturing information, at the LCM prompt:

1. Type **ident**

   LCM displays the following type of information:

```
Part Number:  501-3000-002   X70002e4-0006891
Up-Link Module Part Number: 123-4567-891 X1234567-1234567
Power-up test codes:  00000000 00000000 00000000 00000000
Diagnostic data:  00000000 00000000 fffffffc fffffffc
                  00000000 ff006000
```

4.4 MANAGING THE FN10

Managing the FN10 consists of:

- Disabling and enabling Ethernet ports
- Changing a subnet mask
- Changing a community name
- Setting the baud rate of your terminal connection
- Setting a reboot time

You can use the Local Console Manager (LCM), any of the Cabletron Systems NMSs, or a standard SNMP-based NMS to manage the FN10. Refer to Section 4.1.

4.5 USING LCM TO MANAGE THE FN10

The LCM commands that enable you to manage the FN10 include:

- Disable
- Enable
- Ipaddr
- Community
- Baud
- Reboot

These LCM commands are described in the sections that follow.

4.5.1 Disabling a Port

There can be times when you need to disable a specific Ethernet port, for example, after you have determined that there is faulty equipment. Disabling a port effectively stops all bridging functions for that port. Disabled ports do not accept SNMP packets, and therefore cannot communicate with an NMS.

To disable a port, or port range, at the LCM prompt:

1. Type **`disable <PORT-RANGE>`**

   For example, **`disable 7-9`** would disable ports 7, 8, and 9.

   LCM responds:

```
Port 7: Disabled
Port 8: Disabled
Port 9: Disabled
```

Once an Ethernet port is disabled, it will be disabled until you enable it again. Resetting the FN10 will not enable a port that has been disabled.

If you disable the port through which someone is remotely managing the FN10, that person will not be able to communicate with the FN10. Use the LCM command **`addresses display`** to find the port number you are using to manage the FN10.

4.5.2 Enabling a Port

When you enable an Ethernet port that has been disabled, whatever bridging functions you had previously configured for that port are re-enabled.

To enable a port, or a range of ports, at the LCM prompt:

1. Type **`enable <PORT-RANGE>`**

   For example, **`enable 7-9`** would enable ports 7, 8, and 9.

   LCM responds:

```
Port 7: Enabled, Rip listening
Port 8: Enabled, Rip listening
Port 9: Enabled, Rip listening
```

Entering **`enable <port number>`** for an already enabled FN10 port resets that port's statistics counters.

`Rip listening` means that the FN10 is in listening mode only. No RIP packets are created.

4.5.2.1 noRIP Option

The Routing Information Protocol (RIP) is one of the protocols that allows the FN10 to build an accurate, current routing table. This table includes the networks it knows about, the next hop, and the number of hops to get there. RIP enables you to use an NMS to remotely manage the FN10 through a router.

The **noRIP** option allows you to turn off the routing information that builds the routing table. You would use this option when you are connecting network devices that do not support RIP.

4.5.3 Changing a Subnet Mask

You can optionally set the subnet mask for a port. A subnet mask is a 32-bit address mask used in IP to specify a particular subnet. If the subnet mask is 0.0.0.0, the FN10 automatically converts the displayed mask to the standard default, based on the port's IP address class. (Class A address masks are 255.0.0.0, Class B address masks are 255.255.0.0, Class C address masks are 255.255.255.0.)

To display IP addresses, subnet masks, and MAC addresses of all ports on the FN10 you are managing, at the LCM prompt:

1. Type **ipaddr**

   LCM displays the current IP address table, for example:

```
Port IP Address          Address Mask          MAC Address
  1   192.138.217.1      255.255.255.0      00:40:27:00:06:1f
  2   0.0.0.0            255.0.0.0          00:40:27:00:06:c3
  3   192.138.217.10     255.255.255.0      00:40:27:00:06:3e
  4   0.0.0.0            255.0.0.0          00:40:27:00:03:7a
  5   0.0.0.0            255.0.0.0          00:40:27:00:05:c7
  6   192.138.217.20     255.255.255.0      00:40:27:00:04:4a
  7   192.138.217.50     255.255.255.0      00:40:27:00:06:9e
```

To change the subnet mask, at the LCM prompt:

1. Type **ipaddr <PORT-NUMBER> <IP ADDRESS> <SUBNET MASK>**

   For example, **ipaddr 6 192.138.217.40 255.255.240.0** would set the subnet mask for port 6 to 255.255.240.0. LCM responds by redisplaying the address table.

When you change the subnet mask for a port, you must also enter the IP address for that port. Make sure you enter the IP address for the port correctly; whatever you enter becomes the IP address.

To assign a new IP address, refer to Section 3.1.

4.5.4 Changing a Community Name

A community name is similar to a password. You use the same steps to assign a new community name or to change an existing community name. This sets the MIB variable `sxadminAnyPass`. You can then enter a community name to perform any SNMP *sets*.

To assign a community name, at the LCM prompt:

1. Type **`community`**
2. Enter the old community name.

   If one has not been assigned, you do not need to enter anything. LCM prompts you for the new community name.
3. Enter the new community name.

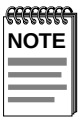
   LCM prompts you to verify the new community name by retyping it.
4. Retype the new community name.

4.5.5 Setting the Baud Rate

You can set the baud rate for your LCM console connection. The options for baud rate include:

- 1200
- 2400
- 4800
- 9600
- 19200

The default rate is 9600.



Make sure that the baud rate you set matches the baud rate setting for the terminal you are using.

To display the current baud rate setting, at the LCM prompt:

1. Type **baud**

   LCM responds:

```
Usage: baud [1200|2400|4800|9600|19200]
   Baud rate is 4800.
```

To change the baud rate setting, at the LCM prompt:

1. Type **baud <baud rate>**

   For example, **baud 9600** would set the baud rate to 9600.

   LCM responds:

```
Baud rate is 9600.
```

4.5.6 Setting a Reboot Time

You can enter the number of seconds the FN10 waits before rebooting. At the LCM prompt:

1. Type **reboot <time interval>**

For example, **reboot 60**

LCM responds:

```
System will be reset in 60 seconds.
```

CHAPTER 5
FN10 FILTERS

One of the most significant features of the FN10 is its powerful user-configurable filtering capabilities. A filter is an instruction to the FN10 to screen data packets based on the criteria you define. Filtering is useful for gathering statistics, implementing security measures, and improving network performance.

The FN10 also supports pseudo filtering. Pseudo filtering provides a unique traffic monitoring capability, including:

- Determining the effect a filter would have, without actually invoking it.
- Monitoring traffic patterns to help determine optimum network design.
- Monitoring potential security threats.
- Evaluating security policies.

You can configure the FN10 to selectively filter network traffic using the following types of filters:

- Bridge Address Table filters
- Port filters

Although proper use of filters can have a positive effect on the network performance, excessive use of filters may degrade network performance. (Refer to Section 5.6.)

5.1 BRIDGE ADDRESS TABLE FILTERS

Bridge Address Table filters use the FN10 Bridge Address Table to determine if there are any filtering flags assigned to a packet's source or destination address. By assigning FN10 Bridge Address Table filter flags, you can selectively filter:

- Traffic to and/or from any station (Media Access Control (MAC) layer address).

- Multicast traffic from any station (MAC layer address). Multicast packets are those destined for more than one address.

Each source address can be assigned one of the following restrictions:

- Filter all packets from this source address.
- Filter all multicast packets from this source address.

You cannot configure Bridge Address Table filters using the Local Console Manager (LCM).

The capacity of the FN10 Bridge Address Table is 8,192 entries. The majority of entries are dynamically learned addresses. However, 200 entries can be static (manually entered).

Table 5-1 shows what a dynamically learned entry in the FN10 Bridge Address Table might look like.

Table 5-1 Representation of an Internal Bridge Address Table Entry

MAC address	Port (segment)	Age	Source filter	Multicast source filter
00:01:02:03:04:05	3	26	OFF	OFF

Where:

MAC address – Indicates the Ethernet address.
Port (segment) – Indicates the physical Ethernet segment port associated with the MAC address. The segment port number is automatically learned for dynamic addresses, but can be manually entered as a static address.
Age – Indicates when a frame from the device was last received by the FN10.
Source filter – Indicates the flags used solely for filtering. They instruct the FN10 to filter (ON) or not filter (OFF) packets generated by specified MAC address.
Multicast source filter – Indicates the flags used solely for filtering. They instruct the FN10 to filter (ON) or not filter (OFF) multicast packets generated by specified MAC address.

With the Bridge Address Table entry shown in Table 5-1, you can use any of the following types of Bridge Address Table filtering:

- Source address
- Source address multicast
- Destination address

5.1.1 Source Address Filter

The source address filtering capability uses the source filter flag, which is a component of each entry in the FN10 Bridge Address Table. When the flag is set to ON, all packets originating from the designated MAC address are filtered. This enables the FN10 to recognize — and ignore — local traffic. Local traffic refers to data packets that only need to travel within one network segment.

5.1.2 Source Address Multicast Filter

The source address multicast filtering capability uses the multicast source filter flag in the FN10 Bridge Address Table.

When this flag is set to ON, all multicast packets originating from the designated MAC address are filtered. This is useful for preventing broadcast traffic from a particular station from being propagated to other network segments.

5.1.3 Destination Address Filter

A destination address filter can be used to discard all traffic destined to a specific MAC address. This type of filter is configured by setting a static address entry for the MAC address and specifying `{null}` as the port assignment. The port assigned by the static entry will take precedence over the port learned by the FN10's learning algorithm.

Destination address filters can be used to create *virtual LANs*. For example, if you want users on Ports 1 and 2 to communicate with each other, and users on Ports 3, 4, and 5 to communicate with each other, but not allow cross traffic between the two groups, you could configure a destination address filter for the broadcast address (i.e., ff:ff:ff:ff:ff:ff), as follows:

- Source Port 1, then forward to Port 2
- Source Port 2, then forward to Port 1
- Source Port 3, then forward to Ports 4 and 5
- Source Port 4, then forward to Ports 3 and 5
- Source Port 5, then forward to Ports 3 and 4

5.2 PORT FILTERS

In contrast to Bridge Address Table filters, which apply to traffic to or from a particular MAC address, Port filters apply to traffic to or from a specific port on the FN10.

Using any of the FN10 management tools, you can assign an **Entry** port one of the following restrictions:

- Filter all packets entering the port, except those from addresses defined as static entries in the FN10 Bridge Address Table.
- Treat all packets with identical source and destination addresses as broadcasts.
- Filter all packets that match all of the fields in the Port filter.

Likewise, you can assign an **Exit** port one of the following restrictions:

- Only allow a certain number of multicast packets every “n” seconds and then stop transmitting.
- Filter a packet destined for this port that matches all of the fields in the Port filter.

Port filters can include multiple filtering conditions. This makes it possible to configure very specific filters. For example, a Port filter could be configured to filter all AppleTalk packets from Port 2 whose destination address is XYZ.

In this example, three filtering conditions are specified. The Port filter could be logically represented as:

Filter packets if:

- They are from Port 2.
- They are AppleTalk packets.
- The destination address is XYZ.

The FN10 allows you to implement up to 100 Port filters (total, for all connected ports). The various types of filtering conditions that can be specified are referred to as *fields*.

5.2.1 Configurable Fields

Port filters can be configured to selectively filter network traffic based on specific **Entry** and **Exit** ports. Entry port filters include filtering conditions on a port that is to receive a packet. Exit port filters include filtering conditions on a port to which the packet is destined.

Each Port filter can contain entries for the configurable fields, with the exception of the *Port/Group Match* and *Port/Group#* fields that are only used with **Exit** port filters. If you do not specify a value for a particular field, that field will not be used.

The **Type** field (**Entry** or **Exit**) must always be specified, since it identifies which traffic flow the FN10 is to observe for filtering. The default is **Entry**.

For the fields defined as **True**, **False**, or **Not Applicable** (**NA**) in the following sections:

- **True** – Means all traffic that matches the field will be filtered.
- **False** – Means all traffic that does not match the field selection will be filtered (inverse filter).
- **Not applicable (NA)** – Means that when the filter is invoked, the FN10 will not check this field.

In addition to the configurable fields, there are two additional options you can use when you configure Port filters:

- Pseudo filtering
- Filter links

5.2.1.1 Pseudo Filtering

Any Port filter can be set to **pseudo** mode. In pseudo mode, the filter generates statistics, counting how many packets meet the filtering criteria. The FN10 does not actually block any traffic.

The pseudo filter option provides unique traffic monitoring capability, including:

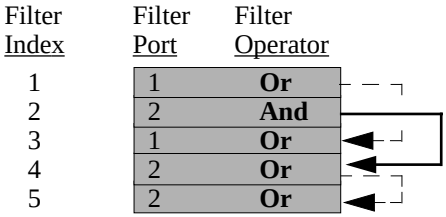
- Determining the effect a particular filter would have, without actually invoking it.
- Monitoring traffic patterns as an aid in determining optimum network design, usage policies, and so on.
- Monitoring potential security threats.

5.2.1.2 Filter Links

Port filters can be logically linked using the Boolean **And**/**Or** operators. Because Port filters are maintained as a table, each Port filter you configure is assigned a Port Filter Table index number. This number is incremented each time a Port filter is added to the Port Filter Table index.

Port filter processing is a one pass, sequential operation. All **And**/**Or** operators apply to the next Port filter in the Port Filter Table index that is assigned the *same* port number and **Entry**/**Exit** value.

For example, if you had the configuration shown below, the **And** operator assigned to Port 2 would apply to the next instance of Port 2, not necessarily the next sequential filter number in the Port Filter Table index.



The Port filter configuration fields are described in Table 5-2.

Table 5-2 Port Filter Configuration Fields

Field	Description	Default
Port	If the filter is for port 1, you do not need to enter anything. If the filter is for another port, enter that number.	1
Type	Either **Entry** – apply the filter to all packets received on the port, or **Exit** – apply the filter before transmitting the packet from the port.	Entry
Port/ Group Match	Either **NA** (not applicable), **True** – filter the packet if the receiving port or group number matches, or **False** – filter the packet if the receiving port or group number does not match. This is valid only if the filter type is **Exit**.	NA
Port/ Group #	Decimal value for the number of the port or group through which the packet entered the FN10 XE. This is valid only if the filter type is **Exit**. Port group numbers start at 25.	NA
Source Range	Either **NA** (not applicable), **True** – filter the packet if the source MAC address is within the range, or **False** – filter the packet if the source MAC address is outside of the range.	NA

Table 5-2 Port Filter Configuration Fields (Continued)

Field	Description	Default
Source Range Start	The starting MAC address for the source range of MAC addresses. If you are filtering on a single source address, enter that address here.	
Source Range End	Ending MAC address for the source range of MAC addresses. If you are filtering on a single address, enter that address here.	
Source Range Mask	MAC address mask to apply to the range of source MAC addresses.	ff:ff:ff: ff: ff:ff
Destination Range	Either **NA** (not applicable), **True** – filter the packet if the destination MAC address is within the range, or **False** – filter the packet if the destination MAC address is outside of the range.	NA
Destination Range Start	Starting MAC address for the destination range of MAC addresses. If you are filtering on a single source address, enter that address here.	
Destination Range End	Ending MAC address, for the destination range of MAC addresses.	
Destination Range Mask	MAC address mask to apply to the range of destination MAC addresses.	ff:ff:ff: ff: ff:ff
Protocol Match	Either **NA** (not applicable), **True** – filter the packet if the protocol type matches, or **False** – filter the packet if the protocol type does not match.	NA
Protocol Type	For all **Ethernet-2**, **802.3**, or specific Ethernet frames. All of the Ethernet hex values are listed in RFC 1060. Some common Ethernet protocol hex values include: 0800 – IP, 0806 – ARP, 6003 – DECnet Phase IV, and 809B – AppleTalk	
Field Match	Either **NA** (not applicable), **True** – filter the packet if the masked value matches, or **False** – filter the packet if the masked value does not match. This option allows you to examine a portion of a packet to set up customized filters to match conditions you specify.	NA

Table 5-2 Port Filter Configuration Fields (Continued)

Field	Description	Default
Field Origin	Either **TYPE**, **IP**, **MAC, or SR** (see Field Offset description). The origin is the field from which the offset count starts.	TYPE
Field Offset	The decimal offset of the portion of the packet to be examined. If the origin is **TYPE**, the field offset value is relative to the end of the Ethernet frame type, regardless of whether or not the frame type is SNAP encapsulated. For example, for IP packets, a field origin of **TYPE** with a field offset of zero indicates the start of the IP header. If the origin is **IP**, then the offset is relative to the end of the IP Header (an offset of zero indicates the portion immediately following the end of the IP Header). If the origin is **MAC**, then the offset is relative to the beginning of the MAC addresses (an offset of zero indicates the start of the destination MAC address). If the origin is **SR**, then the offset is relative to the end of the MAC header, including the Source Routing (SR) header, if present.	
Field Value	The two digit hexadecimal value of each of the eight octets beginning at the origin and offset by the value specified above. The octets must be separated by spaces. This is the value that the filter is using when it does a comparison for a match, for example a MAC address.	
Field Mask	An eight octet mask applied to the packet's eight octets before comparing them to the Field Value specified above. The mask octets must be separated by spaces. This is a mask of the specified Field Value.	
Filter Index	Filter number for this filter. For example, a value of one indicates that this is the first filter in the Filter Table. If you use the default index of 1, any other filters you have previously defined will be renumbered starting with 2. Although filters are assigned to a port, filter indexes are not; they are assigned sequentially to all filters for all ports.	One

When adding or modifying a filter, you must enter both a *Source Range Start* value and a *Source Range End* value. For example:

```
Source Range: [NA] (InRange/OutRange/NA)>inrange
Source Range Start: [00:00:00:00:00:00] >08:00:20:00:00:00
Source Range End: [00:00:00:00:00:00] >00:40:60:0a:10:3e
Source Range Mask: [ff:ff:ff:ff:ff:ff] >ff:ff:ff:00:00:00
```

To filter on a single address, be sure to enter the same address in both the `Source Range Start:` and `Source Range End:` fields.

5.3 USING FILTERS FOR SECURITY PURPOSES

The various types of security restrictions that can be implemented using filters include:

- Restricting access to a network segment – you can configure a filter to prevent any traffic from being forwarded to a specific network segment.
- Restricting access to specific stations – you can use filters to restrict access to specific stations on the network.
- Preventing access by unauthorized users – you can use filters to restrict individual workstations from accessing other network devices.

For each example shown below, the situation is described first, and the objective to be accomplished is explained. Then, how the objective could be accomplished using the FN10 is explained in general terms. In these examples, single letters are used to represent MAC-layer addresses. Actual MAC addresses consist of a string of numbers, (22:14:15:4:5:6).

Example 1: Restricting Access to a Network Segment

The objective in this example is to restrict access for security reasons. Workstations on one network segment (subnet) are to be restricted entirely from access to devices on an adjoining subnet.

In this example, there are three subnets connected by a centrally located FN10 (see Figure 5-1). The subnets are referred to as Manufacturing, Engineering, and Accounting.

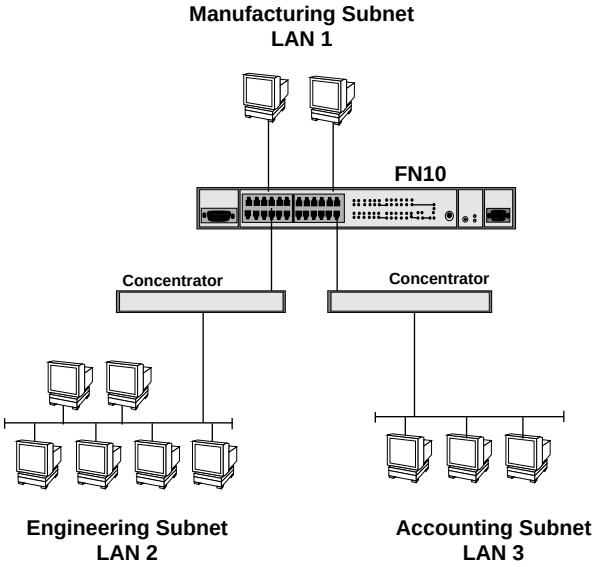


Figure 5-1 Using Filters to Restrict Access to an Adjoining Network Segment

The company wants to allow Engineering and Accounting workstations to access resources on the Manufacturing subnet (**LAN 1**), but wants to prevent users on the Engineering subnet (**LAN 2**) from accessing resources on the Accounting subnet (**LAN 3**). Therefore, the objective is to set up a filter that will block all traffic between LANs 2 and 3, while allowing users on both LANs 2 and 3 to access LAN 1.

For this example, assume that LAN 2 and LAN 3 are connected to ports 2 and 3 on the FN10, respectively. LAN 1 is connected to the ports 1 and 4 on the FN10.

Two Port filters are used to discard any packets from the Engineering subnet destined for the Accounting subnet (LAN 2 to LAN 3), and any packets from the Accounting subnet destined for the Engineering subnet (LAN 3 to LAN 2). Each filter includes:

- The source LAN or port number
- The destination port
- Match flags

The filters are constructed as follows:

- Filter 1: Identifier is port 3 as a destination (i.e., exit)
  Fields are source LAN = 2, Match
- Filter 2: Identifier is port 2 as a destination (i.e., exit)
  Fields are source LAN = 3, Match

Any packet whose source is LAN 3 and destination is port 2 will be filtered. Likewise, any packet whose source is LAN 2 and destination is port 3 will be filtered. However, the filters will not affect user access to the Manufacturing subnet (LAN 1). Therefore, the objective has been accomplished: Users on LANs 2 and 3 (Engineering and Accounting) cannot communicate, but users on either LAN can access LAN 1 (Manufacturing).

This is an example of logical segmenting. In this case, LANs 2 and 3 are distinct physical segments. However, before the filters were implemented, they were able to freely communicate. The filters were used to logically segment the network in such a way that LANs 2 and 3 cannot communicate.

Example 2: Blocking Access to Specific Stations

In this example, a company uses a FN10 to connect two LANs (see Figure 5-2). Three workstations on LAN 2 (the Accounting Subnet) contain sensitive data (workstations F, G, and H). The company wants to prevent users on LAN 1 (the Manufacturing Subnet) from accessing data on these three workstations. Therefore, the objective is to prevent users on LAN 1 from accessing workstations F, G, and H on LAN 2.

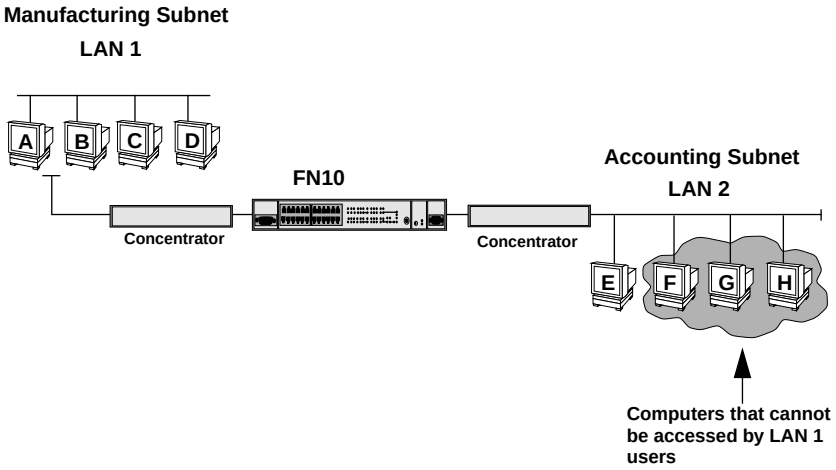


Figure 5-2 Using Filters to Restrict Access to Specific Stations

In this example, a Port filter is configured that instructs the FN10 to discard data packets whose destination address is F, G, or H (the addresses of the workstations containing sensitive data). Therefore, the FN10 will not pass any packets from LAN 1 to LAN 2 if the packet's destination address is F, G, or H.

This filtering example specifies three separate components:

- Traffic from LAN 1
- Traffic destined for addresses F, G, and H on LAN 2
- Match flags for both components

This information is used to configure the filter as follows:

- Filter identifier – port number of the port attached to LAN 2 as a destination.
- Filter fields – destination address F-H (range, match) source LAN = 1 (match).

Note that a match flag is specified for both fields; this instructs the FN10 to filter any packets that match both fields (traffic from LAN 1 and to addresses F-H on LAN 2).

Several methods are available to accomplish this goal. For example, the Port filter could have been specified as follows:

- Filter identifier – port number of the port attached to LAN 1 as a source
- Filter fields – destination address F-H (range, match)

This example is useful for illustrating three basic concepts concerning filters:

- Even though a FN10 is used to join network segments, it can also be used to block selected traffic — or all traffic if desired — between joined segments. The blocking mechanism is the filters you set up.
- Filters can be based upon various criteria: source address, destination address, packet type, and so on. In the example, the filter criteria were source port and destination MAC address.
- A filter can only block (discard) packets which must cross the FN10. The FN10 in the example can only filter traffic that travels from LAN 1 to LAN 2 (or from LAN 2 to LAN 1).

  While a filter can prevent LAN 1 stations from accessing the sensitive-data workstations on LAN 2, it cannot prevent workstation E on LAN 2 from accessing these workstations. The reason is that workstation E is on the same LAN as the sensitive-data computers, and therefore does not need to use the FN10 to access them.

Example 3: Restricting Access to Authorized Users

The example shown in Figure 5-3 is very similar to the previous example. The difference is that access to workstations F, G, and H will not be denied to all LAN 1 users. Instead, only authorized users on LAN 1 will be able to access the sensitive data workstations F, G, and H on LAN 2.

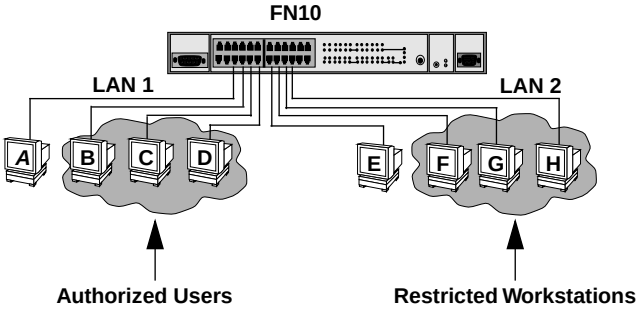


Figure 5-3 Using Filters to Restrict Access to Authorized Users

A Port filter is configured that allows data packets to be sent to the restricted workstations on LAN 2 only if the packet's *source address* is the address of an authorized user on either workstation B, C, or D of LAN 1. The Port filter's components are:

- Source addresses (of authorized users)
- Destination addresses (which identify packets directed to any of the restricted workstations)
- No match flags for both of the above components

The filter is configured as follows:

- Source address field: B, C, or D (LAN 1), no match
- Destination address field: F, G, and H (LAN 2), no match

The No match flag is used in both fields to instruct the FN10 to filter all traffic that does not match both fields.

All packets destined for the restricted workstations on LAN 2 (F, G, or H) are filtered, unless the source address is the address of an authorized user on LAN 1 (B, C, or D).

Note that the FN10 is not storing information designed to identify restricted devices or authorized or unauthorized users. Instead, it is using address information (which it does store) to act on filters that have been configured to meet the desired objective: Restrict access to certain workstations to authorized users.

5.4 USING FILTERS TO ENHANCE NETWORK PERFORMANCE

In many applications, filters can be used to enhance network performance by preventing certain types of traffic which may degrade performance. A filter that defines logical barriers to protect a network segment or segments from conditions that may degrade network performance is referred to as a *firewall filter.*

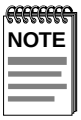
Examples of poor network performance that can be controlled by firewall filters include:

- Unnecessary traffic
- Broadcast storms
- Conflicting applications that occur within a particular network segment

Firewall filters can also be used to help implement fault isolation, error recovery, and security measures.

A firewall filter can be a Bridge Address Table filter or a Port filter. Firewall filters can be configured to:

- Allow only server traffic to be forwarded from LAN A to LANs B and C. (Other traffic would not be forwarded.)
- Prevent a specific type of traffic from being forwarded to a specific network segment. For example, it might be desirable to block DECnet broadcast traffic from a LAN that includes no devices that use DECnet data packets.
- Prevent multicast packets from being forwarded to a specific network segment (localized broadcast storm prevention).



The FN10 multicast storm protection feature may be thought of as a firewall feature, in that it performs a protective blocking function. However, it is not a filter. Multicast storm protection is described in Section 3.10, **Configuring Multicast Storm Protection**.

Example 4: Using a Firewall Filter to Control Multicasts

To optimize network performance, you can configure filters to reduce multicasts (packets broadcast to multiple destinations). In addition, you can prevent multicasts packets of a particular protocol type.

In this example, four LANs are interconnected by a FN10 (see Figure 5-4). The objective is to prevent LAN 1 from sending AppleTalk I multicasts to LANs 2 and 3, yet allow AppleTalk I multicasts to be sent from LAN 1 to LAN 4.

The filter described is a firewall filter; it acts as a barrier to protect the network from a condition that may degrade network performance.

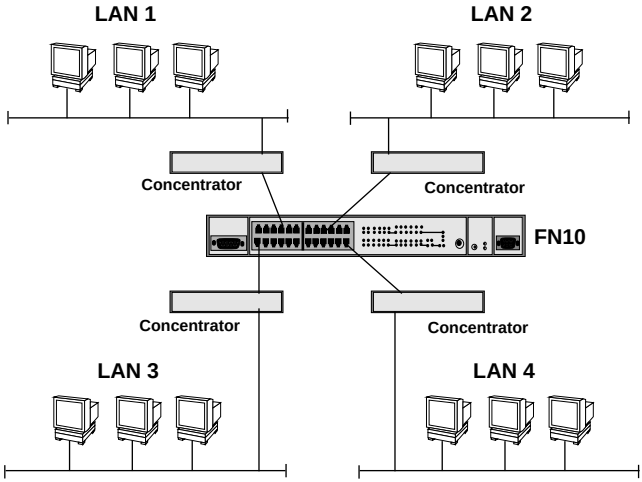


Figure 5-4 Using Firewall Filters to Reduce Multicasts

This filter is configured as follows:

- Filter identifier – port number of the port attached to LAN 2 as a destination (i.e., exit)
- Filter identifier – port number of the port attached to LAN 3 as a destination (i.e., exit)
- Filter fields – protocol type = AppleTalk I, match source LAN = LAN 1, match destination address, match

This filter blocks AppleTalk I multicasts (or all AppleTalk I traffic if the destination address field is omitted) from LAN 1 to LANs 2 and 3, yet AppleTalk I traffic to LAN 4 is permitted because LAN 4 is not specified for filtering.

5.5 CONFIGURING A PORT FILTER

To configure a Port filter, use the Local Console Manager (LCM). The LCM prompts you through the fields for each Port filter you want to configure. If you are adding a Port filter to be used in conjunction with another Port filter, and the filters must be ordered sequentially, use the LCM **`filters display`** command to find the filter index number of the existing Port filter.

After you have configured a Port filter, the LCM display would look something like the example shown below. Your actual display depends on how you have configured your Port filter.

```
Port Number? >1

Index:                          1
Type:                           Entry
Pseudo:                         True
SourceRange:                    True
SourceRangeStart                00:00:00:00:00:00
SourceRangeEnd:                 00:00:00:00:00:00
SourceRangeMask                 ff:ff:ff:ff:ff:ff
DestRange:                      True
DestRangeStart:                 00:00:00:00:00:00
DestRangeEnd:                   00:00:00:00:00:00
DestRangeMask:                  ff:ff:ff:ff:ff:ff
ProtocolMatch:                  True
ProtocolType:                   LLC
FieldMatch:                     True
FieldOrigin:                    IP
FieldOffset:                    0
FieldValue:                     00:00:00:00:00:00:00:00
FieldMask:                      ff:ff:ff:ff:ff:ff:ff:ff
Operator:                       And
PktCnts:                        0
Octets:                         0
LasrSRC:                        00:00:00:00:00:00

Type <cr> to display the next filter ...>
```

See Table 5-2 for information on the configurable fields.

Complete the following steps to configure a Port filter. To accept a default value, press the Enter key.

At the LCM prompt:

1. Type **`filters add`**
2. Enter the port number.

   1 is the default. If the filter is for port 1, you do not need to enter anything; if the filter is for another port, enter that number.

3. Select the filter type.

   Entry is the default. If the filter will be an entry filter, you do not need to enter anything; if the filter will be an exit filter, type **`exit.`**

4. Select whether the filter should be a real filter or a pseudo filter.

   True is the default; meaning the filter will be a pseudo filter. You do not need to enter anything if the filter is to be pseudo. If you want the filter to be a real filter, type **`False.`**

5. Select whether the filter will use a range of source MAC addresses.

   NA is the default; meaning the filter will not use a source range. You do not need to enter anything unless you are using a source range. (If you are not using a source range, go to Step 8.)

   If you are using a source range, type either:

   True – Filter the packet if the source MAC address is within the range.

   False – Filter the packet if the source MAC address is outside the range.

6. Enter the first MAC address in the source range.
7. Enter the last MAC address in the source range.
8. Enter the source range MAC address mask.

   ff:ff:ff:ff:ff:ff is the default address mask. If ff:ff:ff:ff:ff:ff is the mask you want to use, you do not need to enter anything. If you want to use a different mask, enter that value.

9. Select whether the filter will use a destination range of MAC addresses.

   NA is the default; meaning the filter will not use a destination range. You do not need to enter anything unless you are using a destination range. (If you are not using a destination range, go to Step 12.

   If you are using a destination range, type either:

   True – Filter the packet if the destination MAC address is within the range.

   False – Filter the packet if the destination MAC address is outside the range.

10. Enter the first MAC address in the destination range.
11. Enter the last MAC address in the destination range.
12. Enter the destination range MAC address mask.
13. Select whether the filter will use a protocol match.

    NA is the default. You do not need to enter anything unless you are using a protocol match. (If you are not using a protocol match, go to Step 15.)

    If you are using a protocol match, type either:

    True – Filter the packet if the protocol type matches.

    False – Filter the packet if the protocol type does not match.

14. Enter the protocol type to match.
15. Select whether the filter will use a field match.

    NA is the default. You do not need to enter anything unless you are using a field match. (If you are not using a field match, go to Step 20.)

    If you are using a field match, type either:

    True – Filter the packet if the masked value matches.

    False – Filter the packet if the masked valued does not match.

16. Enter the field origin.
17. Enter the field offset.

18. Enter the field value.
19. Enter the field mask.
20. Select the operator.

    Or is the default. You do not need to enter anything if the filter will use the **Or** operator. If you want the filter to use the **And** operator, type **`And`**.

21. Enter the filter number.

    One (**1**) is the default. You do not need to enter anything if the filter number is 1.

    If you want the filter to have an index number other than 1, enter the value you want to use.

LCM displays the filter you entered and prompts you to save it. Enter **y** (Yes) to save the filter, or **n** (No) to cancel it. If you save the filter, it is redisplayed.

5.5.1 Modifying a Port Filter

You modify a Port filter in much the same way as you add one. LCM prompts you through each field. To modify a Port filter, begin with the steps below, then follow the prompts as if you were adding a filter.

At the LCM prompt:

1. Type **`filters modify`**

   LCM prompts you for the filter index (number).

2. Enter the filter index number.

   LCM displays the filter type field and prompts you through the filter fields in the same way as when you add a filter. What you had previously entered becomes the default value and is displayed in brackets [ ]. Make any changes you want following the instructions for adding a filter.

5.5.2 Deleting a Port Filter

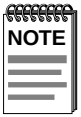
To delete a Port filter, at the LCM prompt:

1. Type **`filters delete`**

   LCM prompts you for the filter index.

2. Enter the filter number.

   LCM responds filter deleted.



All filter indexes are sequential, beginning with the number one. When a filter is deleted, all filters are renumbered so that the filter index remains sequential.

5.6 FILTERING AND PERFORMANCE CONSIDERATIONS

When implementing filters, the FN10 must process packets to determine if they should be filtered. Therefore, the processing that takes place on filters can exact a toll on FN10 throughput (or forwarding) performance.

Typically, if you are using Bridge Address Table filters or a small number of Port filters, they will have little effect on performance. However, a large number of Port filters can reduce the maximum possible forwarding rate. For this reason, filters that are no longer needed should be removed.

CHAPTER 6
FN10 DIAGNOSTICS AND TROUBLESHOOTING

The FN10 incorporates several built-in diagnostic and testing capabilities which are convenient to use and cause minimal or no disruption to the operational network. These capabilities are effective for isolating problems within the FN10 unit. Built-in diagnostic capabilities include:

- System-wide power-up diagnostics, which are run every time the system is powered up or reset.
- Local and remote loopback tests on any of the FN10's 24 Ethernet ports.

All tests can be performed locally or remotely using an in-band or out-of-band Network Management System (NMS).

6.1 POWER-UP DIAGNOSTICS

The FN10 performs an extensive set of diagnostic self-tests whenever any of the following events occurs:

- Power-up
- Reset using the front panel Reset button
- Reset via the NMS (a soft reset)
- Automatic reset in response to a non-recoverable failure

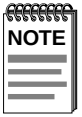
The power-up diagnostics test processors, memory, and other critical hardware components of the FN10. All diagnostic software is stored in non-volatile memory (EPROM).

6.1.1 Power-up LED Sequence

When you power-up the FN10, the following occurs:

1. All LEDs, except for the Port Link LEDs, turn on for one second.
2. The Power (Pwr) LED remains on.
3. The Ready LED starts flashing.
4. After several seconds, the Port Link LEDs turn on briefly.
5. After several more seconds, the Ready LED will stay on, indicating that the power-up diagnostics sequence is complete.

   In addition, the Port Link LEDs will turn on for those ports with good links and the Segment Status LEDs will turn on (or flash) when the selected status condition is present.



If a critical component fails diagnostics, the Ready LED will turn off and the FN10 will attempt to reboot. If the Ready LED does not stay on, contact Cabletron Systems Technical Support. Refer to Section 1.2.

6.1.2 Specific Power-up Tests

The power-up diagnostic tests performed on the FN10 include:

- ROM checksum test
- Instruction/Data memory test
- Memory map test
- Interrupt test
- Packet memory test
- Shared RAM component test
- Ethernet data loopback test

6.1.3 Software Checksum Comparison

When the FN10 reboots, its operational software is verified by a checksum comparison before it is loaded. If the software fails the checksum test due to an interrupted new software distribution procedure, the FN10 will automatically use its backup version of software. A backup version of software is always stored in non-volatile memory.

The operational parameters of the FN10 software are also protected by a checksum comparison. When the FN10 reboots, if the operational parameters of the FN10 fail a checksum test due to a power failure in the midst of a previous update, the FN10 automatically uses its backup version of the parameters.

A backup version of the operational parameters is always stored in non-volatile memory before any update is attempted.

6.1.4 Power-up Diagnostics Results

After completion of the power-up diagnostic sequence, both the Power (Pwr) and Ready LEDs located on the front panel of the FN10 should be on.

6.2 RESPONSES TO FAILURES AT POWER-UP

How the FN10 responds to failures detected during power-up depends on the seriousness of the failure. For example, the FN10 will operate if a non-critical component, such as the out-of-band management port, fails diagnostics. However, in the event of a critical failure, such as a failure of the main element processor, the FN10 will halt execution and will not boot to operational mode.

6.3 DIAGNOSTIC LOOPBACK TESTS

You can perform local and remote loopback tests on any Ethernet port while the FN10 is operational.

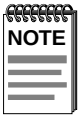
6.3.1 Loopback Tests

Built-in local and remote loopback tests can be used to test individual ports while the FN10 is operational. When in local loopback mode, a port is disconnected from the network. The FN10 generates loopback packets for the port, and the port loops the packets back without sending them onto the network.

During a remote loopback test, the port is in normal operation, sending and receiving packets to the network. The FN10 generates loopback packets which are sent to a particular destination device on the port's network. The destination device echoes the packet back onto the network, and the originating port receives the packet.

For both types of tests, normal operation is indicated when generated packets are received back without errors. For remote loopback tests, the FN10 creates LLC Type 1 test packets for LANs, and Point-to-Point Protocol (PPP) echo-request packets for managing the out-of-band port.

Both types of loopback tests can be initiated by the NMS. The test results are reported to the NMS. Refer to the *Fast Network 10 MIB Reference Guide* for information on the MIB variables.



Loopback testing is automatically performed whenever the FN10 boots. However, there are no LEDs for the loopback tests; the results of these tests must be observed by accurate packet transmission, or read by using an NMS to examine traps.

6.4 STATUS AND ACTIVITY INDICATORS

The front panel of the FN10 includes LEDs that indicate the status or activity of various system components. Figure 6-1 shows the FN10 front panel LEDs and buttons. The LEDs and buttons are described in Tables 6-1 and 6-2.

FN10

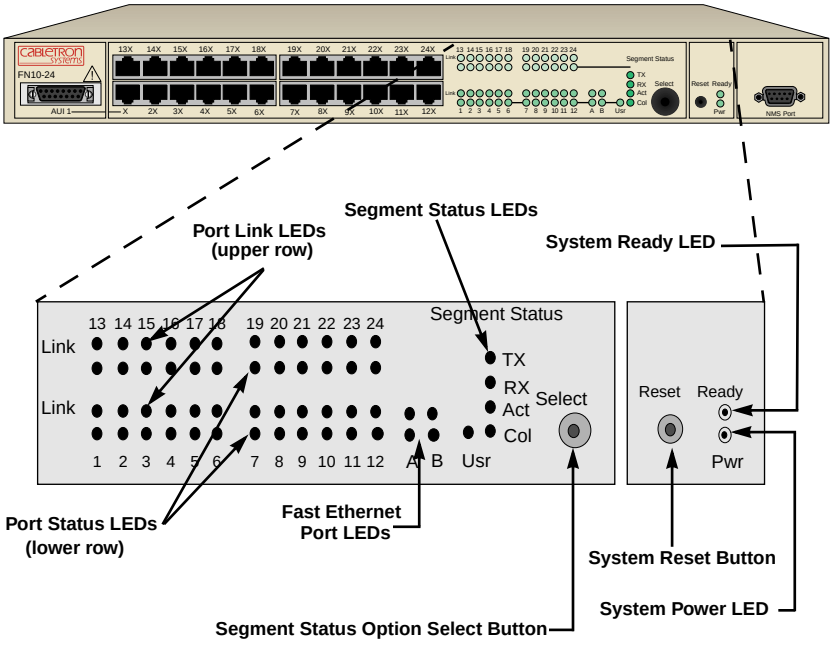


Figure 6-1 FN10 Front Panel LEDs

Table 6-1 Meaning of FN10 LEDs

LED	Meaning
Link (upper level of port LEDs)	On – Indicates the link is good. Off – Indicates there is no link.
Status (lower level of port LEDs)	On/Blinking – Indicates you are monitoring the port for a selected segment status condition. Off – Indicates you are not monitoring the port.
Segment Status TX RX Act Col Usr	 On – Indicates you are monitoring Transmit (TX) activity on all ports. On – Indicates you are monitoring Receive (RX) activity on all ports. On – Indicates you are monitoring Transmit (TX) and Receive (RX) activity on all ports. On – Indicates you are monitoring packet collision on a all ports. On – Indicates you are monitoring transmission and receive errors on all ports.
Ready	On – Indicates the FN10 is operational. Blinking – Indicates the FN10 is running power-up diagnostics. Off – Indicates the FN10 is non-operational.
Pwr	On – Indicates the FN10 is receiving power and the voltage is within the acceptable range. Off – Indicates the FN10 is not receiving power.

If the Ready LED continues to blink after power-up diagnostics are complete, it could mean the FN10 is overheating.

Table 6-2 describes the FN10 buttons.

Table 6-2 Description of FN10 Buttons

Button	Function
Select	Cycles through the Segment Status options (TX, RX, Act, Col, Usr) for all ports. The lower port status LED of the ports you are monitoring is activated based on what function you chose with the Select button.
Reset	Restarts the system software.

6.5 TROUBLESHOOTING

This section lists several situations that could happen while using the FN10, and suggests appropriate action. Because every situation is potentially unique, the corrective actions suggested here should be considered as guidelines only.

6.5.1 FN10 Does Not Power Up

If your FN10 does not power up, check each one of the following:

- Make sure the power source is operational.
- Make sure the power cord is securely connected.

If the FN10 still does not power up, contact Cabletron Systems Technical Support. Refer to Section 1.2 for more information.

6.5.2 Connectivity Problems

- Check for LED abnormalities.
- Check port status using LCM.
- Check for loose port connections.
- Check to see if the number of carrier losses is increasing using LCM. This indicates that the connection is suspect.
- Check to see if the number of total collisions has dramatically increased using LCM.

6.5.3 FN10 Has Rebooted

- Use the LCM `ident` command to check the FN10 diagnostic codes, and call your authorized Cabletron Systems representative.

6.5.4 FN10 Does Not Respond to NMS

- Check the port status using LCM.
- Check to see if the Spanning Tree topology is stable using LCM.
- Check that a pathway to the FN10 exists.
- Verify the FN10's IP address using LCM.

APPENDIX A
TECHNICAL SPECIFICATIONS

A.1 FN10 SPECIFICATIONS

Physical

Height	1.75 in (4.45 cm) (1 *u*)
Width	17 in (43.18 cm)
Depth	15.75 in (40 cm)
Weight	9 lb (4.1 kg)
Installation options	Tabletop or rack-mount

Electrical

Input voltage	Auto-ranging from 100-120, 200-240 Vac
Frequency	50/60 Hz
AC power consumption	80 watts

Connector Ports

12 or 24 RJ45 Ethernet ports (MDI-X)
2 RJ45 Fast Ethernet ports (FE option)
1 AUI D-type, 15-pin female port
1 RS232C D-type, 9-pin female port using Point-to-Point (PPP)
or Local Console Manager (LCM)
2 optional Fast Ethernet Fiber Optic ST ports

Environmental

Operating temperature	5° to 40° C (41° to 104° F)
Relative humidity	0% to 95%, non-condensing

Diagnostic LEDs

Individual port link status (12, 24, or 26 with FE option)
Individual port segment status (12, 24, or 26 with FE option)
Segment status (5), specifying:
- Transmit activity
- Receive activity
- Both Transmit and Receive activity
- Collision
- User-defined

Ready (1)
Power (Pwr) (1)

Bridging Technologies

- IEEE 802.1 Part D
- IEEE802.2 (Logical Link Control)
- IEEE 802.3 (CSMA/CD, 10BASE-T)
- Transparent Bridging with Spanning Tree
- Ethernet Version 2
- EIA RS232C (DTE-to-DCE Interface Specification)
- EIA RS-310-C (Rack-mount Specification)

Address Table Size

8,192 dynamic (learned) entries

Management Support

- MIB II, 802.1d, 802.3, and SMC Enterprise MIB
- Cabletron Systems Local Console Manager (LCM)
- Any SNMP-based network management system

Certification

Safety	UL 1950, CSA C22.2 No. 950 , EN 60950, and IEC 950
Emission	FCC Part 15 Class A, VCCI Class 1, EN 55022 Class A
Immunity	EN 50082-1

A.2 SERIAL CABLE PIN ASSIGNMENTS

For a PC running a Windows terminal connected to the RS232C Network Management Port on the front panel of the FN10, the following serial cable pin assignments are required to manage the FN10 using the Local Console Manager (LCM).

DB-9 (male) to the FN10 (female)	PC DB-9 (female)	25-pin (female)
Pin 2 (Rx)	Pin 2	Pin 3
Pin 3 (Tx)	Pin 3	Pin 2
Pin 5 (Ground)	Pin 5	Pin 7

A.3 10BASE-T PIN ASSIGNMENTS

An Ethernet twisted-pair link segment requires two pairs of wires. Each wire pair is identified by solid and striped colored wires. For example, one wire in the pair might be red and the other wire, red with white stripes.

Connectors

Refer to the diagram below and note how the pins are numbered. Be sure to hold the connectors in the same orientation when connecting the wires to the pins.

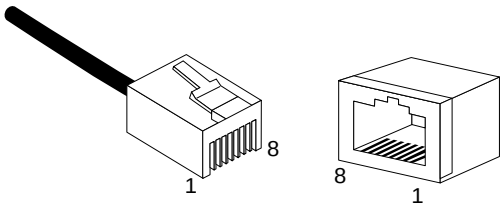


Figure A-1 Connector Pin Numbers

Each twisted-pair link segment must have a male connector attached to both ends. According to the 10BASE-T specification, pins 1 and 2 on the connector are used for transmitting data; pins 3 and 6 are used for receiving data, as shown in Table A-1.

Table A-1 Pin Assignments

Pin	Assignment[a]
1	Tx+
2	Tx-
3	Rx+
6	Rx-

a. The “+” and “-” signs are used to represent the polarity of the two wires that make up each wire pair.

A.4 STRAIGHT-THROUGH WIRING

If the twisted-pair link segment is to join two ports on a switch, and only one of the ports has an internal crossover, the two pairs of wires must be straight-through, as shown in Table A-2.

Table A-2 Straight-through RJ45 Pin Assignments

Hub	Device
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

A.5 CROSSOVER WIRING

Two FN10s can communicate only if the transmitter on one unit is connected to the receiver on the other unit. This reversal, or crossover function, can be implemented either in the wiring or in the device itself. When connecting FN10s, a crossover must be implemented in the wiring. Refer to Table A-3 for crossover pin assignments.

Table A-3 Crossover RJ45 Pin Assignments

FN10	FN10
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

A.6 5 - 4 - 3 RULE

Between any two nodes (i.e., PCs or other stations) on the network, there can be:

- Up to five segments in series
- Up to four repeaters or multi-port hubs
- Up to three populated segments (that is, segments attached to two or more PCs)*

* The remaining two segments are unpopulated; these are known as inter-repeater links or IRLs. This distinction between populated and unpopulated segments is significant for coax networks only.

This rule is completely consistent with the IEEE 802.3 specification, and is meant only to summarize the configuration specification.

APPENDIX B
GLOSSARY

address
A set of characters that uniquely identifies a station, peripheral device, node, or other unit in a network.

address table
A database of device addresses and their associated ports maintained by a switch or bridge for use in making data packet forwarding and filtering decisions.

address table filter
A mechanism for selectively forwarding or discarding (filtering) data that uses address table information to perform relatively simple filtering operations.

agent
Network management software that runs within a managed network device.

alarm
See *trap*.

ANSI
American National Standards Institute – One of several organizations that establishes standards that apply to internetworking.

ARP
Address Resolution Protocol – An auxiliary protocol of the IP layer used to perform dynamic address translation between MAC addresses and internet addresses. Binds IP addresses to specific MAC addresses.

attenuation
The amount of power (or light) lost as power travels through a medium from the transmitter to the receiver. Difference between transmitted and received power, in decibels (dB).

AUI (attachment unit interface)
A standard connector type used for Ethernet connections.

backbone
The major, central transmission path for a network. A backbone usually handles high-volume, high-density traffic. Typically a backbone connects various LANs into an integrated network.

bandwidth
A measure of the amount of traffic a given medium can handle at one time: The communications capacity (measured in bits per second), of a transmission line or of a specific path through a network. Greater bandwidth generally means more information can be sent through a circuit during any given period of time.

BPDU (bridge protocol data unit)
A data unit transmitted as part of the IEEE 802.1d Spanning Tree Protocol. The exchange of BPDUs allows bridges within a network to logically configure the network as a single spanning tree.

bps (bits per second)
The basic unit of data communications rate measurement.

bridge
An intelligent, protocol independent device used to connect similar or dissimilar LANs.

bursty
Adjective used to describe sporadic heavy volumes of network traffic (e.g., bursty traffic).

bypass
Optical or electronic isolation of a station from the network. A bypass situation typically occurs as a result of a station failure or shutdown; the bypass allows the network to function normally, except for the absence of the missing station.

combination port filter
A filter that can include several configurable fields and can be used to filter network traffic in a specific way.

concentrator
A device that provides attachment points for stations that are not connected to the FN10. The concentrator is connected directly to the network; the stations connect to the concentrator.

congestion
A condition where a portion of the network is overloaded with more data than can be transmitted in the desired time period.

CSMA/CD (carrier-sense multiple access with collision detection)
A channel access (contention) method that requires each station to wait for an idle channel before transmitting. In addition, stations are able to detect overlapping transmissions (collisions) and retransmit in the event of a data collision.

data link layer
Layer 2 in the OSI model. Defines frame construction, addressing, error detection, and other services to higher layers.

datagram
Abbreviated and connectionless single-packet message sent from one station to another.

data rate (or speed)
The maximum number of bits of information that can be transmitted per second.

destination address filtering
A process that discards (filters) traffic based on MAC destination addresses.

downstream
Refers to the relative position of a station in a network to another station in the same network. A station is downstream from another station if it receives data after the other station receives data.

dynamic address
An address “learned” by the FN10, as opposed to addresses that are manually entered into the Bridge Address Table. The FN10 “learns” addresses by reading them from the data packets it processes.

EIA (Electronic Industries Association)
Organization that sets standards for electrical interfaces (connectors).

encapsulation
A method for moving messages across networks that use different types of protocols. The message is encapsulated (rather than translated), so it can move across a network that otherwise could not understand its protocol. Encapsulating bridges and switches generally use proprietary encapsulation schemes.

encode
To translate data into a series of electrical or optical pulses that can travel efficiently over a cable or other medium.

entity
An active element within an Open Systems Interconnection (OSI) network layer or sublayer.

extended LAN
A collection of LANs interconnected by protocol-independent bridges or switches.

filter
An instruction to the FN10 to discard certain types of data packets.

filtering rate
A measure (in packets per second) of the FN10's efficiency in examining each frame, comparing it with an address table, and then deciding whether to discard the frame or forward it.

forwarding rate
The rate (in packets per second) at which the FN10 can receive a stream of packets from one network segment, complete all processing, and transmit the packets to another network segment.

frame
A data message that includes a source address, destination address, data, frame check sequence (FCS), and control information.

full wire speed
Refers to packet forwarding at the maximum rate at which data can be transmitted on a given LAN.

ICMP (Internet control message protocol)
An auxiliary protocol of IP used to convey advice and error messages about events in the IP layer.

IEEE (Institute of Electrical and Electronic Engineers)
International professional society which issues networking and other standards. The IEEE created the 802 family of LAN standards:

IEEE 802.2
The data link layer standard; used with IEEE 802.3, 802.4, 802.5, and other LAN/WAN protocols.

IEEE 802.3
The physical layer standard that uses the CSMA/CD access method on a bus topology LAN.

IEEE 802.6
Standard for metropolitan area networks (MANs) currently under development.

initialization
Transition of a device or network from startup state to operational state.

intelligent bridge/switch
A bridge/switch that is able to identify source and destination addresses.

internet
A large communications infrastructure composed of wide and local area networks. A generic reference to a network built using internetworking technology.

Internet
A large collection of connected networks which use TCP/IP. (Also referred to as the DARPA Internet, NSF/DARPA Internet or the Federal Research Internet.)

internetworking
The linking of one or more networks to facilitate communication across networks.

interoperability
The ability of equipment from multiple vendors to exchange information using standardized protocols.

IP (Internet protocol)
IP is the basic datagram protocol used at the network layer of the TCP/IP stack.

ISO (International Standards Organization)
An organization that creates, controls and publishes standards.

jitter
Clocking deviation on a network.

Kbps (kilobits per second)
1,000 bits per second.

LAN (local area network)
A network that interconnects a variety of devices (computers, printers, servers, and so on), within a limited geographical area. A LAN typically connects devices within a building or campus.

link-loss budget
Each connection (link) in an optical system results in a certain amount of signal strength loss. Link-loss budget refers to the process of calculating link loss for the entire system. If the total link loss exceeds a certain limit, the system will not function.

LLC (logical link control)
A part of the data link layer of the OSI model that defines the transmission of a frame of data between two stations (with no intermediate switching nodes).

LMA (local management agent)
Software running on a network device to control the device in terms of network management functions.

local traffic
Traffic within a given network segment.

MAC (media access control)
The data link layer sublayer responsible for scheduling, transmitting, and receiving data on a shared medium local area network.

mask
Specified a subset of a larger set of data to be included for comparison and analysis. For example, in switch filtering, a mask might be configured to include only the first four address bits as the basis for filtering decisions.

Mbps (megabits per second)
1 million bits per second.

MIB (management information base)
A collection of objects unique to a specific device that can be accessed via a network management protocol. The FN10 has its own MIB.

multicast
Packets destined for more than one address.

multicast (broadcast) storm
Excessive multicast packet traffic, typically generated by a faulty device. Multicast storms can cause severe network performance problems.

network
Interconnected computer systems, terminals, and data communication facilities. A network must have at least three endpoints and may have any number of links and nodes.

node
Any device connected to a communication network, for example a computer, workstation, printer, server, concentrator, bridge, and switch.

OSI (Open Systems Interconnection)
Refers to the OSI reference model, a logical structure for network operations. OSI is the internationally accepted framework of standards for internetwork communication.

packet
A group of bits including data and control elements arranged in a specific format that are transmitted and switched as a composite whole. Control elements include a source address, destination address, frame control and status indicators, and a Frame Check Sequence (FCS).

PDU (protocol data unit)
The portion of a datagram that contains the data associated with a particular protocol.

peer-to-peer
Term used to describe data transmission between entities in the same sublayer of the OSI model.

physical layer
Layer 1 of the OSI model. Defines and handles the electrical and physical connections between systems.

power budget
The difference between transmit power and receiver sensitivity, including any safety margins.

PPP (point-to-point protocol)
A protocol for transmitting datagrams (IP or MAC packets) over a serial point-to-point link (e.g., the out-of-band management port).

pps (packets per second)
Unit of measure used to express packet data throughput. 18 pps is approximately equal to 9600 bps.

propagation delay
The time it takes for a signal to travel across a network.

protocol
A set of rules used by computers and related devices to communicate with each other.

protocol suite
A group of protocols related to a common framework.

RARP (reverse address resolution protocol)
A protocol that binds MAC addresses to specific IP addresses.

RISC (Reduced Instruction Set Computing)
A data processing technology in which functions are performed using the least possible number of instructions to yield very fast processing.

segment
When two or more networks are interconnected to form an internetwork, the original networks are referred to as segments.

service
A set of functions offered to a user by a provider.

SNMP (simple network management protocol)
A TCP/IP protocol for communication between a network management system and a network device.

source address filtering
A switch or bridge function that forwards or rejects data, depending on the data's source address.

static address
Addresses manually entered into the Bridge Address Table (as opposed to those automatically learned by the FN10).

STP (spanning tree protocol)
A protocol that ensures that only one path will be used between two devices; prevents active loops (multiple paths to devices), by closing redundant paths. With STP operating, a redundant link serves as a backup link only if a normal path fails.

switch
An intelligent, protocol independent device used to connect similar or dissimilar LANs.

symbol
The smallest signaling element used by the MAC sublayer. Each symbol corresponds to a specific sequence of code bits to be transmitted by the physical layer.

synchronous transmission
A transmission technique in which an uninterrupted block of data is transmitted, using no redundant information such as stop and start bits to identify the beginning and end of a unit of data.

TCP/IP (transmission control protocol/Internet protocol)
Internetworking protocols sometimes referred to as the Internet suite of protocols.

topology
The arrangement of devices and cable paths that make up a network.

translating bridge
A bridge that can pass data between LANs that use different protocols.

translation
Modification of data packets from one type of network so they can be used on a different type of network (e.g., Ethernet to FDDI translation).

trap
Alarm; notification of an event that has occurred on a network. Some alarms require intervention or action by the network administrator; some are merely informational.

UDP (user datagram protocol)
A TCP/IP protocol for the connectionless transport layer.

upstream
Refers to the relative position of a station in a network to another station in the same network. A station is upstream from its neighbor if it receives data before its neighbor receives the data.

WAN (wide area network)
A communication network that spans a large geographic area.

INDEX

T

V

W