IBM 8250 Multiprotocol Intelligent Hub

SA33-0213-04

Token Ring Management Module Installation and User's Guide

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page xv.

Fifth Edition March 1996

The information contained in this manual is subject to change from time to time. Any such changes will be reported in subsequent revisions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

IBM France
Centre d'Etudes et de Recherches
Service 0798 - BP 79
06610 La Gaude
France

- FAX: (33) 93.24.77.97
- EMAIL: FRIBMQF5 at IBMMAIL
- IBM Internal Use: LGERCF at LGEPROFS
- Internet: rcf_lagaude@vnet.ibm.com

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Parts of information in this guide are reprinted with the permission of 3Com Corporation.

Contents

Chapter 1. Introduction

Chapter 2. Designing Your Network

Chapter 3. Unpacking and Installing the Module

Chapter 4. Preparing the TRMM Command Interface

Chapter 5. Using TRMM Features

Chapter 6. Using RMON to Monitor the Network

Chapter 7. Troubleshooting

Chapter 8. Downloading TRMM Firmware

Appendix A. Specifications

Appendix B. MIB Groups

Index

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send these inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, New York 10594, U.S.A.

CE European Community Marking

The CE marking has been applied to this product, meaning its compliance to the following directives:

- EMC Directive 89/336/EEC and amendment 93/31/EEC
- Low Voltage Directive 73/23/EEC

Electronic Emissions Notices

Federal Communications Commission Notice

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 generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

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.

Industry Canada Compliance Statement

This Class A digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformite aux normes d'Industrie Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Japanese Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the 1st Class category (information equipment to be used in commercial or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment aimed at preventing radio interference in commercial and 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, and so on.

Read the instructions for correct handling.

Korean Communications Statement

This device has been approved for business purpose with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange this device for a non-business purpose.

New Zealand Statement

Attention: This is a Class A product. In a domestic environment, this product may cause radio interference in which case you may be required to take adequate measures.

Trademark and Service Marks

The following terms, denoted by an asterisk (*), used in this publication, are trademarks or service marks of IBM Corporation in the United States or other countries:

IBM*	AIX NetView/6000	AIXwindows
RISC System 6000	NetView	PS/2
AS/400	Nways	

The following terms, denoted by a double asterisk (**), used in this publication, are trademarks of other companies:

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

DEC, DECnet, VT100, and LAT are trademarks of Digital Equipment Corporation.**

Hayes is a registered trademark of Hayes Microcomputer Products.**

OSF/Motif, OSF, and Open Software Foundation are trademarks of the Open Software Foundation.

TriChannel is a registered trademark of 3Com Corporation.**

ProComm is a registered trademark of DATASTORM TECHNOLOGIES, INC.**

DATASTORM is a trademark of DATASTORM TECHNOLOGIES, INC. **

Safety

This product meets IBM* safety standards.

For more information, see the *IBM Telecommunication Products Safety Handbook*, GA33-0126.

Product Page/Warranties

The following paragraph does not apply to the United Kingdom or to any country where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

Statement of Limited Warranty

The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you originally purchase for your use, and not for resale, from IBM or an IBM authorized reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Machines are subject to these terms only if purchased in the United States or Puerto Rico, or Canada, and located in the country of purchase. If you have any questions, contact IBM or your reseller.

Machine - 8250 Token Ring Management Module

Warranty Period* - One Year

Elements and accessories are warranted for three months. Contact your place of purchase for warranty service information.

Production Status

Each Machine is manufactured from new parts, or new and serviceable used parts (which perform like new parts). In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's warranty terms apply.

The IBM Warranty

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. IBM calculates the expiration of the warranty period from the Machine's Date of Installation. The date on our receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period, IBM or your reseller will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine. IBM or your reseller will specify the type of service.

For a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Some of these transactions (called "Net-Priced" transactions) may include additional parts and associated replacement parts that are provided on an exchange basis. All removed parts become the property of IBM and must be returned to IBM.

Replacement parts assume the remaining warranty of the parts they replace.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair or replace it (with a Machine that is at least functionally equivalent) without charge. If IBM or your reseller is unable to do so, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at **1-800-IBM-SERV (426-7378)**. In Canada, call IBM at **1-800-465-6666**. You may be required to present proof of purchase.

Depending on the Machine, the service may be 1) a "Repair" service at your location (called "On-site") or at one of IBM's or a reseller's service locations (called "Carry-in") or 2) an "Exchange" service, either On-site or Carry-in.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced.

It is your responsibility to:

1. Obtain authorization from the owner (for example, your lessor) to have IBM or your reseller service a Machine that you do not own;
2. Where applicable, before service is provided:
    a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
    b. secure all programs, data, and funds contained in a Machine,
    c. inform IBM or your reseller of changes in a Machine's location, and
    d. for a Machine with exchange service, remove all features, parts, options, alterations, and attachments not under warranty service. Also, the Machine must be free of any legal obligations or restrictions that prevent its exchange; and

3. Be responsible for loss of, or damage to, a Machine in transit when you are responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

Misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible may void the warranties.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HOWEVER, SOME LAWS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES. IF THESE LAWS APPLY, THEN ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

In Canada, warranties include both warranties and conditions.

Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part (including fundamental breach) or other liability (including negligence and misrepresentation), you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages, IBM is liable only for:

1. Bodily injury (including death), and damage to real property and tangible personal property; and

2. The amount of any other actual loss or damage, up to the greater of $100,000 or the charge for the Machine that is the subject of the claim.

Under no circumstances is IBM liable for any of the following:

1. Third-party claims against you for losses or damages (other than those under the first item listed above);

2. Loss of, or damage to, your records or data; or

3. Economic consequential damages (including lost profits or savings) or incidental damages, even if IBM is informed of their possibility.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

This warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

About This Book

This guide is designed to help customers understand the features, indicators, and installation procedure for the IBM 8250 Token Ring Management Module (also referred to as TRMM). Information on troubleshooting and diagnostics is included for operation verification.

Who Should Use This Book

This guide is intended for the following people at your site:

- Network Manager or Administrator
- System Manager or Administrator.

How to Use This Book

This guide contains the following chapters and appendixes:

Chapter 1, Introduction — Presents the key features and management functions of the TRMM.

Chapter 2, Designing Your Network — Provides maximum trunk lengths for 4 Mbps and 16 Mbps networks and shows an example of a WAN configuration using the TRMM. This chapter also describes the management capabilities of the TRMM in a typical Token Ring configuration.

Chapter 3, Unpacking and Installing the Module — Provides illustrated procedures for installing the Advanced board onto the Basic board and for installing the TRMM into the 8250 Multiprotocol Intelligent Hub. It also describes the front panel indicators (LEDs), the Reset button, Ring-In/Ring-Out connectors, and the RS-232 serial port connector.

Chapter 4, Preparing the TRMM Command Interface — Explains how to configure the TRMM to manage a Token Ring network. Configuration options include terminal settings, default system values, and configuring the TRMM for communication with SNMP-based management systems.

Chapter 5, Using TRMM Features — Explains how to use TRMM features including BootP, scheduling and scripting, and thresholds. This chapter also describes how to monitor your Token Ring network using the SHOW commands.

Chapter 6, Using RMON to Monitor the Network — Explains how to use the TRMM to administer RMON remote network monitoring functions.

Chapter 7, Troubleshooting — Provides help in isolating and correcting problems that may arise during installation and during normal operation.

Chapter 8, Downloading TRMM Firmware — Explains how to perform out-of-band and in-band downloads to load new software to the Flash or Boot EPROM in your TRMM.

Appendix A, Specifications — Provides technical specifications for the Basic and Advanced versions of the TRMM, such as the electrical and environmental specifications. Also included are Token Ring cable connector requirements.

Appendix B, MIB Groups — Lists the MIB-II and IBM* MIB groups that are supported in Version v4.00.

Index

Document Conventions

The following document conventions are used in this guide.

Text Conventions	Example
User Input	In the Agent Information Form, enter `MIS` in the New Contact field.
System Output	After pressing the Apply button, the system displays the message `Transmitting data`.
Path Names	Before you begin, read the overview file located in the directory **/usr/snm/agents/readme.txt**.
User-substituted Identifiers	In the command above, substitute ***<rem_name>*** with the name of the remote machine.
Keyboard	[ENTER]
Text Emphasis	Ensure that you press the Apply button *after* you add the new search parameters.
Note	Indicates that the information is important.
Warning	Indicates that a condition may damage software or hardware.
Caution	Indicates that a condition may threaten personal safety.

Automatic Update Service

The *Automatic Update Service* (AUS) subscription is a simple and cost-effective way of ensuring that your hardware modules are up-to-date with the latest microcode functions and improvements. Available on a 3-year subscription basis, AUS subscriptions cover all your feature modules with independently upgradable microcode components. With AUS subscriptions, you automatically receive the newest versions of microcode when they are made available.

Two types of subscriptions are available to accommodate your needs:

Single: Subscription for a single feature module.

Site: Subscription for as many modules (of the same type) as needed in one building or campus with a unique mailing address where 8250 modules are installed. This subscription covers modules that are already installed, as well as those ordered during the subscription period.

Improved Decision Making

With the 3-year subscription, it is easy to predict the annual cost of upgrading your network with the latest microcode functions. Also, because you always have the latest version of management modules, fewer planning considerations are required when ordering new media and interconnect modules.

Asset Protection

The automatic distribution of the latest microcode versions ensures that your hardware is always up-to-date with the latest set of functions, thereby expanding the life of your network and reducing compatibility problems.

Connectivity Improvements

With the latest version of microcode in place, your management and interconnect modules are automatically upgraded with the latest performance and configuration improvements, as well as new bridging and routing features.

Network Operations Productivity

The AUS subscription ensures that the modules (of a given type) in your network are kept at the same level of microcode, therefore making network operations simpler and more consistent. Also, with the latest version of the management module installed, the network manager can perform configuration and problem management for all the newly-announced hub components and modules without restrictions.

For more information about the *Automatic Update Service*, contact your IBM marketing representative or your authorized reseller.

Where to Find Further Information

The following documents supply background information:

Case, J., Fedor, M., Scoffstall, M., and J. Davin, *The Simple Network Management Protocol*, RFC 1157, University of Tennessee at Knoxville, Performance Systems International and the MIT Laboratory for Computer Science, May 1990.

Rose, M., and K. McCloghrie, *Structure and Identification of Management Information for TCP/IP-based Internets*, RFC 1155, Performance Systems International and Hughes LAN Systems, May 1990.

IBM Management Information Base (MIB) commands that enable you to manage IBM SNMP-based products are available over the Internet on an anonymous FTP server. Updates to these MIBs and additional MIBs are released as new IBM products are introduced.

To access Internet versions:

1. FTP to `venera.isi.edu` or `128.9.0.32`.
2. Enter the login name `anonymous`.
3. Enter your full Internet e-mail address as the password.
4. Change to the mib directory using the `cd /mib` command.
5. List the contents of the directory using the `ls -l` command and use **Ctrl-S** to pause the display to view the available IBM MIB entries. Use **Ctrl-Q** to continue the display.
6. Copy the IBM MIB files to your current directory using the appropriate command. For example, `get ibm-hub-mib.txt`.
7. To exit the FTP session, invoke the quit command.

If no access to the Internet library is available, contact your IBM marketing representative.

Chapter 1. Introduction

This chapter presents an overview of the 8250 Token Ring Management Module at Version v4.00 for the Basic (FC 3823) and Advanced (FC 3884) versions. It describes the module's key features and management capabilities.

This chapter contains the following sections:

- 8250 Token Ring Management Module
- Theory of Operation
- Network Management Access
- Network Management Functions
- Backplane Architecture

8250 Token Ring Management Module

The 8250 Token Ring Management Module (TRMM) is a single-slot module designed to work with IBM 8250 Multiprotocol Intelligent Hubs. The TRMM provides connection to an IEEE 802.5 Token Ring (LAN), enabling you to fully manage and control a Token Ring network.

In addition, the TRMM includes:

- Monitoring and control capabilities which allow you to configure and check status on all Token Ring, Ethernet, and FDDI modules
- Ring-In/Ring-Out ports to allow you to extend your network to other devices

8250 Token Ring Management Module Versions

The 8250 Token Ring Management Module come in two versions:

- Basic (Feature Code 3823)
- Advanced (Feature Code 3884)

TRMM Basic Version

You can use the TRMM Basic version in any 8250 Multiprotocol Intelligent Hub. The major features of the TRMM Basic version include:

- Compliance with industry standards such as IEEE 802.5, TCP/IP, TELNET, SNMP, and TFTP
- Monitoring and reporting of key Token Ring network fault statistics
- In-band and out-of-band network management
- Dynamic network monitoring and control
- Automatic detection of faults and failures

- Automatic detection and resolution of station beaconing, with the TRMM automatically disabling the port to prevent corruption of the entire ring
- Scripts, which enable you to create a command file by specifying a list of management commands to execute
- Scheduling, which allows you to execute scripts at a specific time of day
- Assignable through software to one of seven separate Token Ring backplane networks
- Support of TriChannel** architecture and fault tolerance capabilities
- Address-to-port security

TRMM Advanced Version

You can use the TRMM Advanced version in any 8250 Multiprotocol Intelligent Hub. The TRMM Advanced version includes all of the features of the Basic version plus:

- Port groups which allow user-defined port groups to be enabled or disabled with a management command.
- Threshold feature that enables you to define network, port, and station thresholds. When the threshold is exceeded, an alarm is sent to the management station.
- Enhanced traffic statistic and performance monitoring capabilities.
- Token Ring RMON MIB support.

Theory of Operation

The TRMM can be installed into any slot in the hub and can communicate with all other modules in the hub using a dedicated control bus as shown in Figure 1-1.

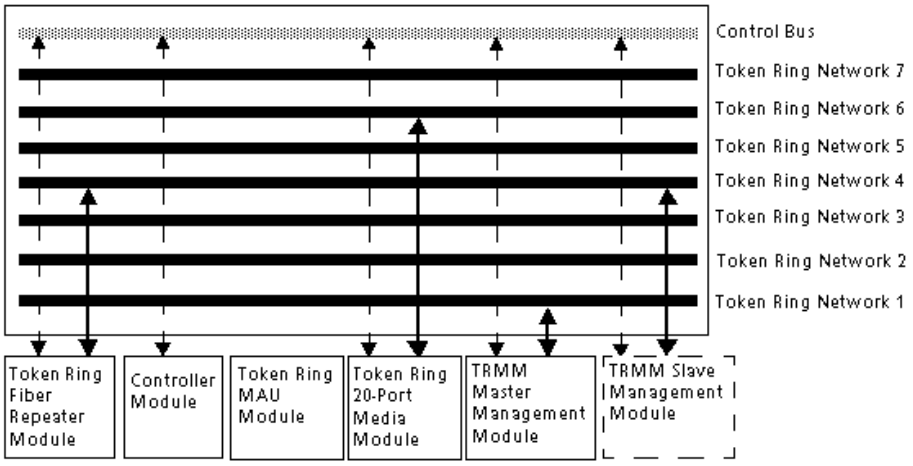


Figure 1-1. TRMM Communication in 8250 Multiprotocol Intelligent Hub

As with media modules installed in the 8250 Multiprotocol Intelligent Hub, the TRMM is assigned using management commands to a network on the hub backplane. The configuration capacity of the TRMM is protocol-independent, enabling you to configure all Token Ring modules as well as Ethernet and FDDI modules.

In addition, using the control bus, the TRMM can configure and check status on *all* modules in the hub, even if they are assigned to different networks, or are isolated from the backplane.

Master and Slave TRMMs

If you have modules assigned to different Token Ring networks in a hub, you should use multiple TRMMs to track real-time statistics on the individual networks. For configuration management, however, only one TRMM in the hub can be the master TRMM. All other TRMMs are considered slaves.

A slave TRMM can collect statistics and listen to traffic on the network to which it is assigned. Because the slave TRMM does not have *control* of the control bus, it cannot configure modules or detect faults. The slave module takes over as master if the master TRMM fails, thus providing fault tolerance for hub management. You can configure the slave module to re-assign itself to a network in the event it becomes master.

The network administrator assigns a mastership priority level between 1 and 10 to each TRMM. Because all TRMMs are factory set with priority level 10, the first TRMM you install automatically becomes master for that hub. If you want the first TRMM to remain master, change the mastership priority of all other TRMMs you install to a lower value.

It is important to note that if a TRMM and an Ethernet Management Module (EMM) are present in the same hub, the TRMM must have a higher mastership priority for beacon recovery to work. If an FDDI Management Module is installed in the same hub, it must be master.

TRMM Network Control

When you install a TRMM into a hub for the first time and it becomes master, it automatically learns and saves the configuration of all existing modules and their ports. The TRMM provides all of the features you need to configure, monitor, and control your Token Ring network at the network console.

The TRMM also enables you to configure 8250 Ethernet and FDDI modules, which gives you the flexibility to handle multiple protocols and media types in a single, managed hub.

TRMM Features

The TRMM provides the following features to maximize security and minimize the risk of losing module and port configuration settings:

- All known modules installed in an 8250 Multiprotocol Intelligent Hub *after* a TRMM has been installed will have all ports disabled and isolated to prevent unapproved connections. The one exception is when a module is unknown to the TRMM, in which case it will be configured from its DIP switch settings.
- You can implement port security by assigning a MAC address to a specific port, and then enabling the security feature for that port. In the event another device is connected to that port, the TRMM disables the port. The TRMM supports up to four MAC addresses per port.
- If you remove any module from the hub and then re-install it (or install another module of the same type) in the same slot, the TRMM automatically configures the module to the last settings saved for that module.
- If you replace a TRMM with another TRMM, the newly installed TRMM automatically learns all module and port configurations. However, you will need to re-enter terminal and device configuration information.
- If hub power fails, the TRMM "remembers" the configuration last saved. Therefore, when power is restored, none of the pre-failure configuration information is lost.

Network Management Access

The TRMM provides both in-band and out-of-band network management access:

- In-band — The TRMM provides:
  - A built-in SNMP (Simple Network Management Protocol) agent. The agent enables you to manage TRMMs through SNMP-based network management systems.
  - TELNET support. TELNET support is based on a fully compliant TCP/IP stack. The TRMM supports up to four simultaneous incoming TELNET sessions.
- Out-of-band — You can connect an ASCII terminal to the RS-232 port on the module faceplate and manage the TRMM using the command-line interface.

Network Management Functions

The TRMM provides management and control capabilities in eight major areas:

- **Configurations** — When logged in under the administrator password, you can configure the TRMM, Token Ring network, modules, ports, trunks, and terminal settings.
- **Fault, Performance, and Traffic Statistics Monitoring** — Typical terminal management systems report statistics only when you request them. You can set the TRMM to continuously monitor and report key statistics by invoking the MONITOR command. The statistics on the screen are updated periodically to give a snapshot of the network.

  The Advanced TRMM also provides the thresholding feature, which enables you to specify thresholds for network, station, or port counters. When a threshold is exceeded, a trap is sent to the terminal or management workstation.

  The Advanced TRMM also offers RFC 1271 and RFC 1513 RMON support.
- **Beaconing Recovery Capability** — The TRMM senses a beaconing port through automatic detection and resolves the situation by disabling the faulty port. The faulty port is bypassed to maintain the integrity of the ring.
- **Security Control** — The TRMM provides two important security features that prevent unauthorized access to devices on the network:
  - Address-to-port security
  - Two-level password protection

  In addition, the Advanced TRMM provides the Port Group feature, which allows you to enable or disable user-defined port groups with one management command.

- **In-band and Out-of-Band Download** — The TRMM provides both in-band and out-of-band download features. An in-band download is performed using TFTP (Trivial File Transfer Protocol). The out-of-band download is performed using Xmodem software and a connection to the RS-232 serial port on the front panel of the TRMM.

- **SNMP Support** — SNMP (Simple Network Management Protocol) is a protocol defined by the Internet community. The TRMM acts as an agent in an SNMP managed environment to respond to SNMP requests and generate SNMP traps.

- **TELNET Support** — The TELNET command enables you to log in remotely to any TRMM on the network and manage it from a remote TRMM. You can also manage a TRMM from a workstation with TELNET support.

- **Mapping** — The TRMM provides an important mapping feature that keeps a detailed topological map of each Token Ring module in the 8250 Multiprotocol Intelligent Hub. The information in this map can be displayed using the SHOW NETWORK_MAP TOKEN_RING command and its options.

Backplane Architecture

The 8250 Multiprotocol Intelligent Hub's unique backplane architecture allows you to create multiple Token Ring, Ethernet, and FDDI networks in one hub. The hub supports the following configurations:

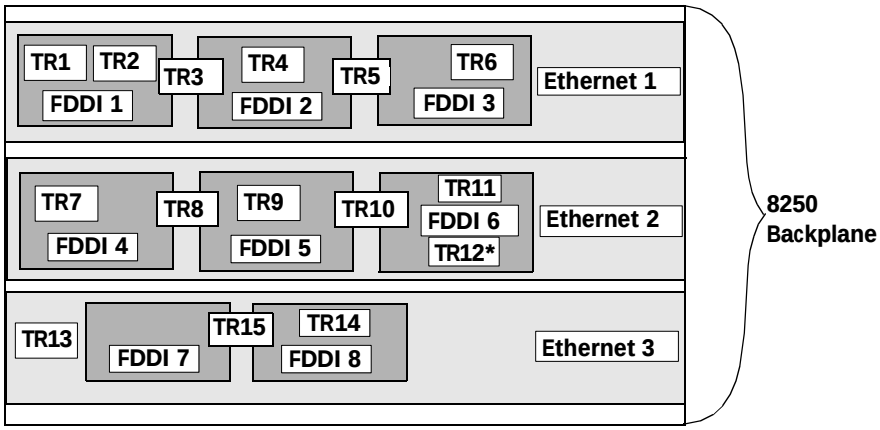
- Three separate Ethernet networks and one isolated network
- Seven backplane Token Ring networks and one isolated network
- Four FDDI networks and one isolated network

Figure 1-2 illustrates how Ethernet, Token Ring, and FDDI networks coexist on the hub backplane. Note in Figure 1-2 that Ethernet networks and paths correspond. That is, the Ethernet_1 network is always allocated to Ethernet path 1, the Ethernet_2 network is always allocated to Ethernet path 2, and the Ethernet_3 network is always allocated to Ethernet path 3.

Token Ring and FDDI networks and paths do not correspond:

- Token Ring — There are 7 available Token Ring *networks* and 15 Token Ring *paths*.
- FDDI — There are 4 available FDDI *networks* and 8 FDDI *paths*.

The master management module dynamically allocates the best possible path currently available for your configuration.



*** TR12 overlays part of FDDI 6, but it does not affect the Ethernet 2 path.**

Figure 1-2. TriChannel Backplane Architecture Assignments

Table 1-1, Table 1-2, and Table 1-3 provide reference charts for configuring Ethernet, Token Ring, and FDDI networks in one hub. These tables define which networks paths are removed when certain network paths are used. Refer to these charts to determine the number and types of different protocol combinations you can have in one hub.

You may want to issue the SHOW NETWORK PATHS command before and after you configure networks to modules or ports to display which network paths are in use.

As shown in Table 1-1, Ethernet_3 is the best Ethernet network selection to use in a mixed-protocol environment because it affects the least amount of Token Ring and FDDI network paths.

Table 1-1. Ethernet Backplane Combination Reference Chart

Ethernet Paths	Token Ring Paths	FDDI Paths
Ethernet 1 removes	Token Ring 1 Token Ring 2 Token Ring 3 Token Ring 4 Token Ring 5 Token Ring 6	FDDI 1 FDDI 2 FDDI 3
Ethernet 2 removes	Token Ring 7 Token Ring 8 Token Ring 9 Token Ring 10 Token Ring 11	FDDI 4 FDDI 5 FDDI 6
Ethernet 3 removes	Token Ring 12 Token Ring 13 Token Ring 14 Token Ring 15	FDDI 7 FDDI 8

Table 1-2. Token Ring Backplane Combination Reference Chart

Token Ring Paths	Ethernet Paths	FDDI Paths
Token Ring 1 removes	Ethernet 1	FDDI 1
Token Ring 2 removes	Ethernet 1	FDDI 1
Token Ring 3 removes	Ethernet 1	FDDI 1 FDDI 2
Token Ring 4 removes	Ethernet 1	FDDI 2
Token Ring 5 removes	Ethernet 1	FDDI 2 FDDI 3
Token Ring 6 removes	Ethernet 1	FDDI 3
Token Ring 7 removes	Ethernet 2	FDDI 4
Token Ring 8 removes	Ethernet 2	FDDI 4 FDDI 5
Token Ring 9 removes	Ethernet 2	FDDI 5
Token Ring 10 removes	Ethernet 2	FDDI 5 FDDI 6
Token Ring 11 removes	Ethernet 2	FDDI 6
Token Ring 12 removes		FDDI 6
Token Ring 13 removes	Ethernet 3	
Token Ring 14 removes	Ethernet 3	FDDI 8
Token Ring 15 removes	Ethernet 3	FDDI 7 FDDI 8

Table 1-3. FDDI Backplane Combination Reference Chart

FDDI Paths	Ethernet Paths	Token Ring Paths
FDDI 1 removes	Ethernet 1	Token Ring 1 Token Ring 2 Token Ring 3
FDDI 2 removes	Ethernet 1	Token Ring 3 Token Ring 4 Token Ring 5
FDDI 3 removes	Ethernet 1	Token Ring 5 Token Ring 6
FDDI 4 removes	Ethernet 2	Token Ring 7 Token Ring 8
FDDI 5 removes	Ethernet 2	Token Ring 8 Token Ring 9 Token Ring 10
FDDI 6 removes	Ethernet 2	Token Ring 10 Token Ring 11 Token Ring 12
FDDI 7 removes	Ethernet 3	Token Ring 15
FDDI 8 removes	Ethernet 3	Token Ring 14 Token Ring 15

Chapter 2. Designing Your Network

This chapter contains configuration information that will help you to plan your Token Ring network. This chapter contains the following sections:

- Beaconing Recovery Capability
- Source Routing
- General Configuration Information
- Cable Types and Ring Speeds
- Maximum Number of Stations
- Maximum Copper Trunk Lengths
- Sample TRMM Configuration
- Example of TRMM Management

Beaconing Recovery Capability

The IEEE 802.5 Token Ring standard specifies that when a station detects a problem with the ring, it sends out a beacon that includes the address of its upstream neighbor. A *beacon* is a frame sent by a station indicating that it has stopped receiving signals from its upstream neighbor. (This condition could be due to a hard error, such as a station with an incorrect ring speed attaching itself to the ring, or a faulty cable.) The ring is said to be *beaconing* if a station sends a beacon frame.

A beaconing station sends out beaconing frames every 20 milliseconds. A beacon frame contains:

- The beaconing station's source address
- The local broadcast address (C0 00 FF FF FF FF)
- An indication of the beacon type (for example, signal loss)
- The address of the upstream neighbor in the NAUN field (Nearest Active Upstream Neighbor)

Note: The beacon frame is sent as a broadcast address. All stations are aware that the ring is beaconing.

Beacon recovery reacts to beaconing conditions as follows:

- **Station receives eight consecutive beacon frames with its own address in the NAUN field —** The station removes itself from the ring by wrapping the transmit pairs and receive pairs of the lobe cable. It then performs a test on itself and its lobe cable. During this self-check, the station sends thousands of frames to itself. If any of the frames are corrupted, the station stays off the ring. If the station is functional, it re-attaches itself to the ring.

- **Station configured for an incorrect ring speed —** The station does not receive the beacon frames and remains on the ring. The downstream neighbor continues to send out beaconing frames because it still cannot receive a signal. Because the beaconing protocol cannot resolve this problem, the TRMM must intervene.

  To maintain the integrity of the ring, the TRMM waits for the station to remove itself from the ring. If the ring is not repaired and the TRMM determines the faulty station is connected to a port in the hub, it disables the port, thus removing the faulty station from the ring. If the TRMM determines that the faulty station exists external to the hub (that is, connected through trunks), it wraps the external trunks that connect the faulty station to the hub. The TRMM re-enables the trunks in less than 10 seconds to check if the beaconing has been resolved externally. If not, it leaves the trunk disabled.

Note: The TRMM can shut down a beaconing port only for modules that reside in the same hub as the TRMM *and* on the same Token Ring network.

- **Device does not support beacon recovery —** TRMM provides the SET TRUNK EXTERNAL_BEACON_RECOVERY NON_EXIST command, which should be issued in a multi-hub environment when an external trunk is connected to a device that does not support beacon recovery. This command enables the TRMM to determine the order in which trunks will be re-enabled in the beaconing process. If the trunk continues to beacon, the TRMM will segment it rather than segmenting the entire ring.

Source Routing

In a transparent bridged network, the end stations have no knowledge that bridges exist. To the end stations there appears to be one large network that can be addressed. In a source routing bridged environment, however, the end stations require knowledge of the bridges between themselves and the remote stations.

The TRMM can be an end station in a source routing bridged environment. It has local tables in memory of source routing paths for remote stations, and these tables are automatically updated. No user input or intervention is required to run in a source routing environment.

General Configuration Information

The TRMM offers front panel connection with a pair of non-repeated copper Ring-In/Ring-Out ports. The copper Ring-In/Ring-Out connections can be used for interconnecting IBM Token Ring MAU Modules or external multistation access units (MAUs) such as the IBM 8228 MAU.

Use only Shielded Twisted Pair (STP) cable on the copper Ring-In/Ring-Out ports. Unshielded Twisted Pair (UTP) cable may appear to work, but can cause intermittent mapping and beacon recovery problems. UTP is not supported for use with the Ring-In/Ring-Out ports.

The copper ports can also be used to connect hubs that are in the same wiring closet. If the copper trunks are used, verify that the copper Ring-In port's network map parameter is set to:

- *external* when connecting hubs or other devices outside (external) to the hub
- *internal* when connecting modules within (internal) the hub

Note: It is not recommended that the copper Ring-In/Ring-Out ports be used for connectivity between wiring closets. You should use the fiber ports on the 8250 Token Ring Fiber Repeater Module (Feature Code 3822) for connectivity between wiring closets.

The TRMM configures Fiber Repeater Modules and Token Ring Media Modules over the backplane by assigning the modules to the same network using internal communication paths. This method is preferred over using the copper Ring-In/Ring-Out ports because it eliminates the possibility of cable problems or accidental disconnections, and allows reconfiguration using software commands.

Warning: Do not connect a TRMM and an 8250 Token Ring Fiber Repeater Module (Feature Code 3822) using both the copper Ring-In/Ring-Out ports and the backplane simultaneously. This is an invalid configuration and will segment the ring into two distinct rings.

Address-to-Port Mapping Limitations

In some configurations, stations that are directly connected to ports in a IBM hub may incorrectly appear to the TRMM as *external* stations. (External indicates that the station is connected to another hub or MAU, and is connected to the ring with copper or fiber trunks.)

In this situation, stations are identified as external when a TRMM is separated from them by two or more external trunk connections (fiber or copper), even though the stations are connected directly to the hub. When stations are external, the beacon recovery feature and the port security feature may not function properly for these ports.

This mapping condition occurs only when two or more trunks are used on two or more modules (for example, using two repeaters, regardless of whether they are in consecutive slots, with at least one trunk used on each module). This condition does not occur if two trunks are used on a single repeater within the ring configuration.

Assigning TRMMs to Networks

The order in which you assign Token Ring modules to a network can assist in proper address-to-port mapping. You should assign modules consecutively, beginning with the module in slot 1.

Once the modules are assigned to Token Ring networks, use the SHOW NETWORK_MAP TOKEN_RING LOGICAL command to verify whether *internal* (directly connected) MAC stations are mapped incorrectly to an external designation, or mapped correctly to a slot/port designation. The SHOW NETWORK_MAP TOKEN_RING LOGICAL command displays information about ring topology and also identifies which port is the active monitor.

If you suspect that an external address-to-port limitation exists, use the SHOW NETWORK_MAP TOKEN_RING PHYSICAL command to observe the order of trunk and backplane connections. This command shows the physical links between ports on all connected Token Ring modules in the hub.

Mapping Examples

Figure 2-1 shows a sample hub configuration, followed by two examples of the SHOW NETWORK_MAP TOKEN_RING PHYSICAL command displays. Both displays report the physical ordering of modules according to the sequence in which the modules were assigned to Token Ring network 1.

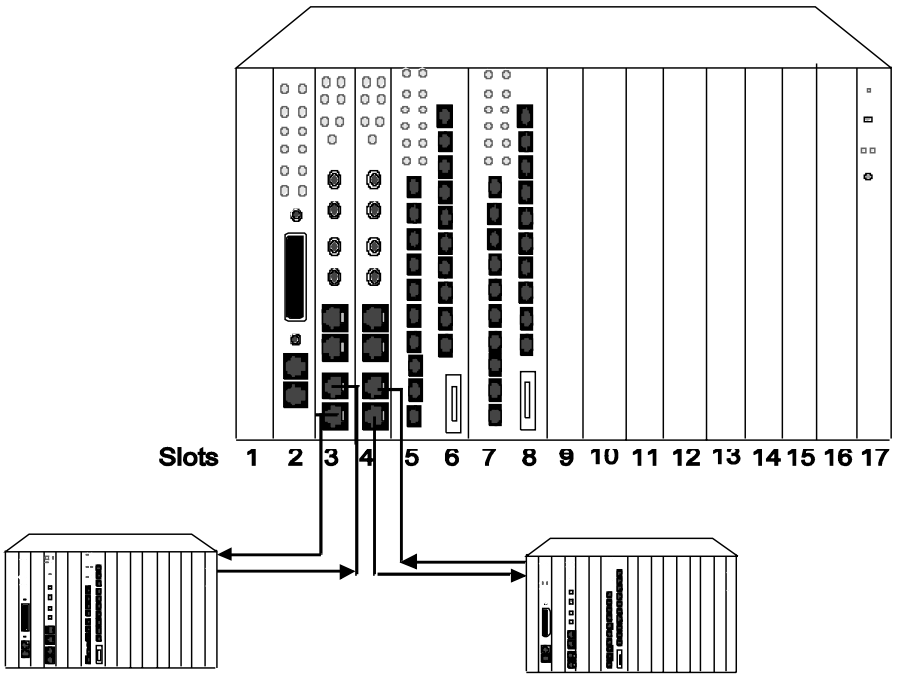


Figure 2-1. Address-to-Port Mapping Example

In this example, the modules are assigned to Token Ring network 1 in the following sequence:

```
8250> set module 4 network token_ring 1
8250> set module 8 network token_ring 1
8250> set module 2 network token_ring 1
8250> set module 3 network token_ring 1
8250> set module 6 network token_ring 1
```

The SHOW NETWORK_MAP TOKEN_RING PHYSICAL command displays the modules in the following order:

```
8250> show network_map token_ring physical

Physical wiring map for modules in TOKEN_RING_1:

Upstream       Connection       Downstream
Slot ID        Type             Slot ID
-------        ----------       -----------
External       Fiber            4
4              Copper           External
External       Copper           4
4              Backplane        8
8              Backplane        2
2              Copper           External
External       Copper           2
2              Backplane        3
3              Fiber            External
External       Fiber            3
3              Copper           External
External       Copper           3
3              Backplane        6
6              Backplane        4
4              Fiber            External
```

If the fiber and/or copper trunks are used on each repeater, the TRMM will not be able to map the stations to ports on the 3821T module in slot 6. This occurs because the TRMM is separated upstream and downstream from the 3821T module by external trunks.

Using the same configuration in Figure 2-1, the modules are assigned to Token Ring 1 in the following order:

```
8250> set module 2 network token_ring 1
8250> set module 3 network token_ring 1
8250> set module 4 network token_ring 1
8250> set module 6 network token_ring 1
8250> set module 8 network token_ring 1
```

The SHOW NETWORK_MAP TOKEN_RING PHYSICAL command displays these modules in the following order:

```
8250> show network_map token_ring physical

Physical wiring map for modules in TOKEN_RING_1:

Upstream       Connection       Downstream
Slot ID        Type             Slot ID
-----------------------------------------
External       Fiber            4
4              Copper           External
External       Copper           4
4              Backplane        6
6              Backplane        8
8              Backplane        2
2              Copper           External
External       Copper           2
2              Backplane        3
3              Fiber            External
External       Fiber            3
3              Copper           External
External       Copper           3
```

If the fiber and/or copper trunks are used on each repeater, the TRMM is able to map the stations on both 3821T modules. The TRMM can map the stations because it is not separated upstream and downstream from the media module ports.

Cable Types and Ring Speeds

Cable type and length requirements vary depending on whether your network ring operates at 4 or 16 Mbps, and by the cable type you use:

- If you are designing a 4 Mbps network that you do not want to upgrade to 16 Mbps, use the 4 Mbps cable configuration rules.
- If you are designing a 16 Mbps network, or a 4 Mbps network that you plan to upgrade to 16 Mbps at a later time, use the cabling configuration rules for 16 Mbps networks.

For cabling configuration rules, refer to the appropriate media module installation and operation guide or the *8250/8260/8285 Planning and Site Preparation Guide* (Document Number GA33-0285).

Maximum Number of Stations

The 1989 IEEE 802.5 standard for Shielded Twisted Pair (STP) networks recommends that no more than 250 stations be connected to a single ring. The *IEEE Recommended Practices for Use of Unshielded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4 Mb/s* specifies that no more than 72 stations be connected to a single ring. The TRMM counts as one station.

Although no IEEE standard currently governs the use of UTP cable for 16 Mbps networks, IBM recommends a maximum of 150 stations. Note that a mixed configuration of modules using STP and UTP in a 4 Mbps network should comply to the UTP standard of 72 stations.

In general, when implementing Token Ring networks it is desirable to configure the rings with fewer than the specified maximum number of stations. Bridges may be used to interconnect smaller rings into a single logical network.

The 8250 Multiprotocol Intelligent Hub does not support the use of fan-out devices that expand a lobe port to allow multiple connections. These devices will invalidate the TRMM's network map and port statistics.

Connecting Rings With Bridges

A Token Ring LAN (local area network) can consist of one or more rings connected by bridges. Bridges can be used to connect more than 250 attaching devices into a single network.

Users from the same department or similar groups can be assigned to the same ring, yet still have access to other resources that are on rings to which their ring is bridged. In a bridged LAN, all of the users have access to each other by passing frames across the bridges and on rings until the destination address has been reached.

Maximum Copper Trunk Lengths

The maximum recommended copper Ring-In/Ring-Out trunk lengths vary depending on ring speed, the number of hubs on the ring, and the type of lobe cable being used. You should use only STP cable on the copper trunks to provide the necessary shielding which protects the integrity of the trunk path (that is, decreasing susceptibility to external noise sources).

Table 2-1 and Table 2-2 define the maximum copper trunk lengths for 4 Mbps networks and 16 Mbps networks, respectively. For example, if you are using STP *lobe* cable to connect two hubs on a 4 Mbps network, you will need to limit your *trunk* length to 355 meters to ensure data integrity. This example is illustrated in Figure 2-2.

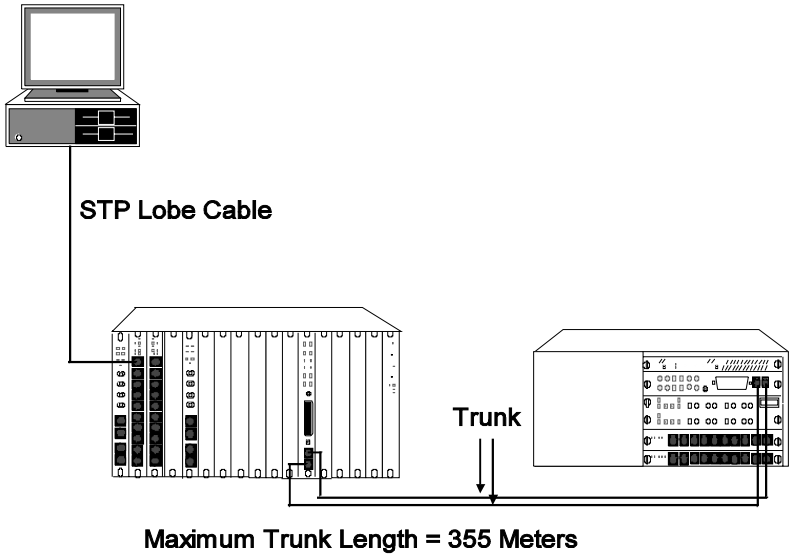


Figure 2-2. Maximum Trunk Length Using STP Lobe Cable Example

Table 2-1. Maximum Trunk Lengths for 4 Mbps Networks

Number of Hubs/ MAUs	Maximum Trunk Lengths (in meters) Using:			
	STP Lobe Cable	UTP Level 5 Lobe Cable	UTP Level 4 Lobe Cable	UTP Level 3 Lobe Cable
2	355	264	264	205
3	336	245	245	186
4	318	227	227	168
5	300	209	209	150
6	282	191	191	132
7	264	173	173	114
8	245	155	155	95
9	227	136	136	77
10	209	118	118	59
11	191	100	100	41
12	173	82	82	23
13	155	64	64	5
14	136	45	45	
15	118	27	27	
16	100	9	9	
17	82			
18	64			

Table 2-1. Maximum Trunk Lengths for 4 Mbps Networks (Continued)

Number of Hubs/ MAUs	Maximum Trunk Lengths (in meters) Using:			
	STP Lobe Cable	UTP Level 5 Lobe Cable	UTP Level 4 Lobe Cable	UTP Level 3 Lobe Cable
19	45			
20	27			

Table 2-2 identifies maximum *trunk* lengths for 16 Mbps networks using STP *lobe* cables.

Table 2-2. Maximum Trunk Lengths for 16 Mbps Networks

Number of Hubs/MAUs	Maximum Trunk Lengths (in meters) Using:		
	STP Lobe Cable	UTP Level 5 Lobe Cable	UTP Level 4 Lobe Cable
2	111	29	16
3	102	20	7
4	93	11	
5	84	2	
6	76		
7	67		
8	58		
9	49		
10	40		
11	31		
12	22		
13	13		
14	4		

The trunk lengths specified are based on lobe lengths of 100 meters or less. The recommended trunk lengths are based on the 22 dB maximum attenuation allowance specified by the IEEE 802.5 standard.

For example, if you are using STP cable to connect five hubs on a 4 Mbps network, you need to limit your trunk length to 300 meters to ensure data integrity. Multiplying 2.2 dB (where 2.2dB = loss/100m of cable) x 6 (300

meters for the transmit path + 300 meters for the receive path = 600 meters) equals 13.2 dB.

This loss is well below the 22 dB set by the 802.5 standard, and allows adequate margin for communication between stations with 100 meter lobe lengths. This calculation also includes adequate margin for losses incurred by other devices and when a break occurs in the network and the backup path must be used.

Sample Valid Configuration

Figure 2-3 provides an example of a valid configuration using the rules outlined in the previous section. In this example, three hubs and one external MAU are connected using the copper trunk connections. For a 4 Mbps network, the maximum trunk length for connecting four hubs and MAUs using STP cable is 318 meters, as defined in Table 2-1. If you add the cable lengths shown in Figure 2-3, the total trunk distance is 245 meters. Thus, the configuration is valid.

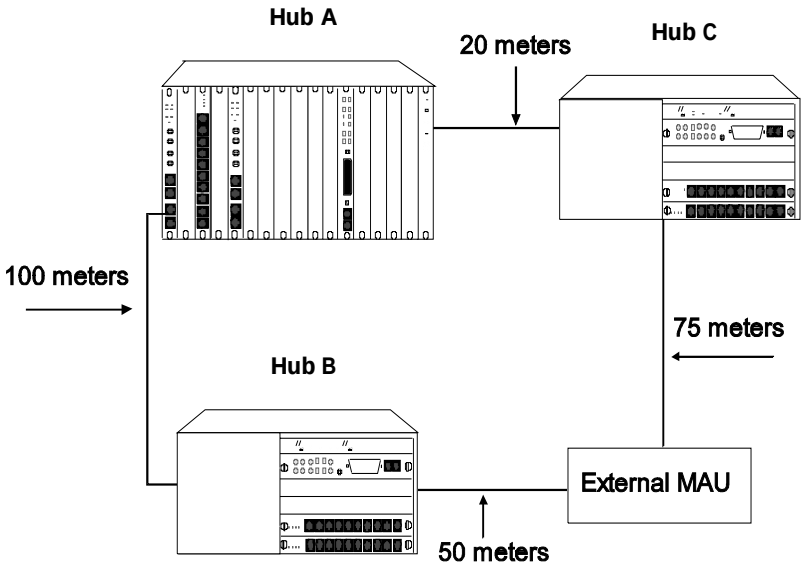


Figure 2-3. Valid Token Ring Configuration

Sample TRMM Configuration

Figure 2-4 illustrates a WAN configuration with a TRMM installed in each hub. The TRMMs can be managed from an SNMP workstation application, such as the IBM Nways* Campus Manager LAN, using a graphical user interface or from a host with TCP/IP and TELNET protocols.

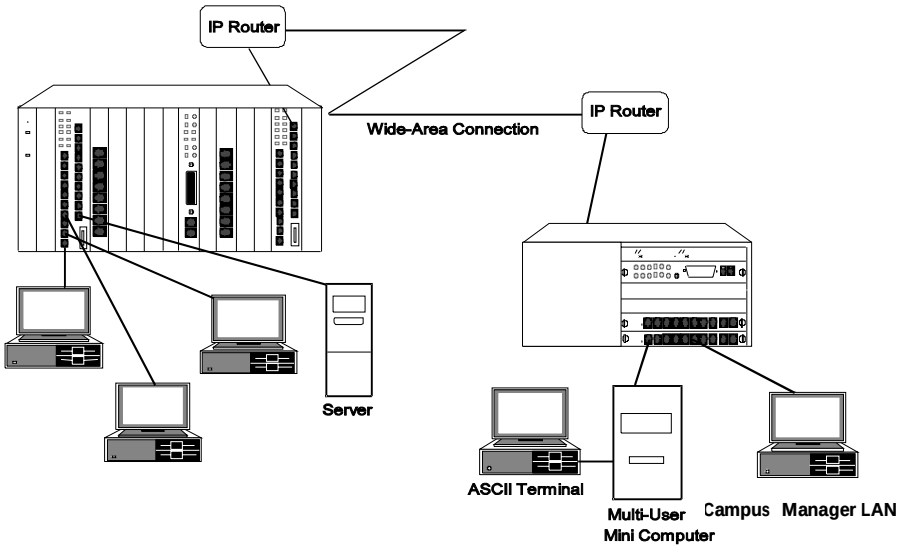


Figure 2-4. TRMMs in a WAN Configuration

Example of TRMM Management

This section describes how the TRMM manages a multi-hub, multi-ring configuration, and the limits of the configuration. General TRMM configuration information is presented first, followed by an explanation of TRMM management illustrated by Figure 2-5.

Token Ring modules can be grouped together with two parameters:

- Whether or not they are in the same ring
- Whether or not they are in the same hub

In this example, a *group* of Token Ring modules is defined as a set of modules that are in the same hub *and* in the same ring.

A TRMM can configure any media modules (that is, Token Ring, Ethernet, and FDDI) that are in the same hub. It cannot configure media modules that are in a different hub. To configure media modules that are in a different hub, you must log in to the second hub using TELNET.

A TRMM can gather statistics for all stations on the ring to which it is assigned. To associate the station statistics to port statistics, however, a TRMM must also be located in the same hub as the ports for which statistics are gathered. The TRMM's beacon recovery capability enables it to shut down a beaconing port only for modules in its group (that is, modules in the same hub and ring as the TRMM).

Figure 2-5 shows three 8250 Multiprotocol Intelligent Hubs with four Token Ring networks and one Ethernet network. The following sections discuss each ring and hub. Each section discusses how the TRMM:

- Controls the ring
- Performs configuration management
- Records statistics
- Performs beaconing recovery

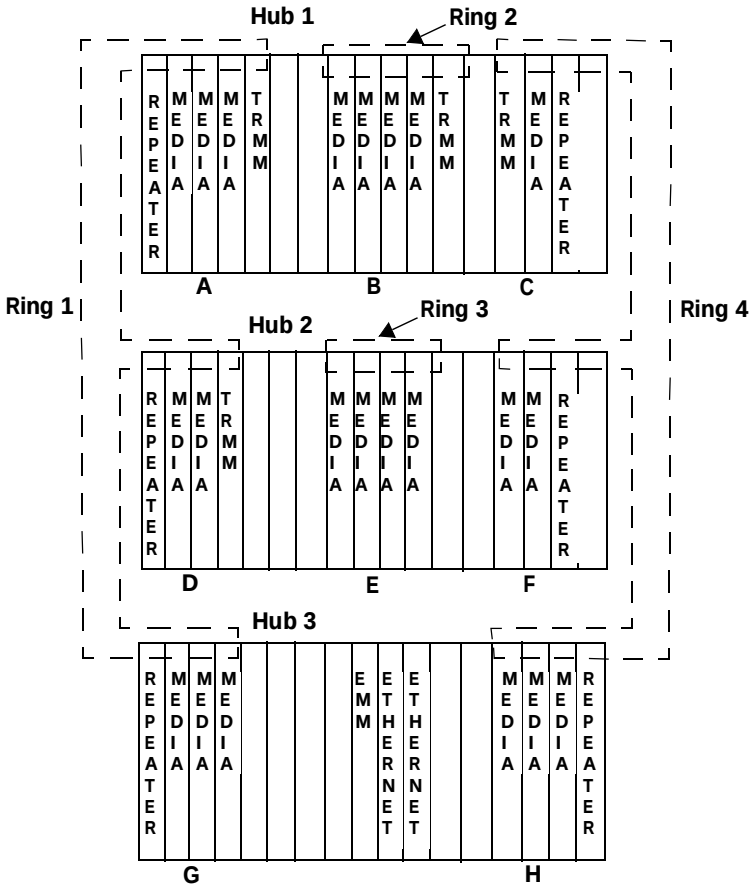


Figure 2-5. TRMM Management With Three Hubs and Four Rings

In general, the TRMM provides the hub labeled Hub 1 with the maximum management capability. By installing a TRMM for each ring in Hub 1, you will receive statistics for each station in addition to per-port statistics. Each TRMM in a ring provides beaconing recovery for that ring.

Description of Token Ring 1

In Figure 2-5, Token Ring 1 spans all three hubs (hubs). It consists of the groups of modules labeled A, D, and G.

Configuration Management

The modules in group A are configured by one of the three TRMMs in Hub 1 (whichever is hub master). The modules in Group D are configured by the TRMM in Hub 2. The modules in Group G are configured by the EMM in Hub 3.

Statistics

The modules in Group A have statistics kept per station by the TRMM in Group A and the TRMM in Group D. Additionally, the TRMM in Group A can associate the counts on a per-port basis for the media modules in Group A (but not Group D or G). Remember that in order to obtain *per-port* statistics, the TRMM must be located in the same hub as the media modules.

The modules in Group D have their statistics kept per station by the TRMM in Group A and the TRMM in Group D. The TRMM in Group D can associate the counts on a per-port basis for the media modules in Group D only (not Group A or G).

The modules in Group G have their statistics kept per station by the TRMM in Group A and the TRMM in Group D. Note that no management module has the ability to associate per-port statistics with the stations attached to the media modules in Group G.

In addition to error statistics, the Advanced TRMM also reports traffic statistics.

Beacon Recovery

The TRMM in Group A will disable a beaconing port for the modules in Group A. The TRMM in Group D will disable a beaconing port for the modules in Group D. A beaconing port in Group G will not be disabled because no TRMM exists in that group.

Description of Token Ring 2

In Figure 2-5, Token Ring 2 is completely contained within Hub 1. The ring consists of the group of modules labeled B.

Configuration Management

The modules in Token Ring 2 are configured by one of the three TRMMs in Hub 1 (whichever is hub master). This is the case even if the master TRMM is not in Token Ring 2. A TRMM master has configuration control for all media modules in its hub.

Statistics

The modules in Token Ring 2 have their statistics kept per station by the TRMM in Token Ring 2. Additionally, the TRMM in Token Ring 2 can associate the statistics on a per-port basis for all of the media modules in Token Ring 2.

Beacon Recovery

The TRMM in Token Ring 2 will disable a beaconing port within that group.

Description of Token Ring 3

In Figure 2-5, Token Ring 3 is completely contained within Hub 2. The ring consists of the group of modules labeled E.

Configuration Management

The modules in Token Ring 3 are configured by the TRMM in Group D.

Statistics

The modules in Token Ring 3 have no statistical reporting capabilities. This is because a TRMM is *not* assigned to Token Ring 3.

Beacon Recovery

A beaconing port that occurs within Token Ring 3 will not be disabled because no TRMM exists on that ring.

Description of Token Ring 4

In Figure 2-5, Token Ring 4 spans all three hubs. It consists of the groups of modules labeled C, F, and H.

Configuration Management

The modules in group C are configured by the master TRMM in Hub 1. The modules in Group F are configured by the TRMM in Hub 2 (Group D, which is part of Token Ring 1). The modules in Group H are configured by the EMM in Hub 3.

Statistics

The modules in Group C have their statistics kept per station by the TRMM in Group C. Additionally, the TRMM in Group C can associate the statistics on a per-port basis for the media modules in Group C only (not Groups F or H).

The modules in Group F and Group H have their statistics kept per station by the TRMM in Group C. No management module has the ability to associate the statistics on a per-port basis with the stations attached to the media modules in Group F or H.

Beacon Recovery

The TRMM in Group C will disable a beaconing port for the modules within that hub. A beaconing port will not be disabled for the modules in Group F or in Group H because no TRMM exists on that ring.

Chapter 3. Unpacking and Installing the Module

This chapter describes how to install the TRMM and verify its operation. It contains the following sections:

- Precautionary Procedures
- Unpacking Procedure
- Advanced Board Installation
- Installing the Module
- Connecting Copper Ring-In/Ring-Out Ports
- Verifying Operation
- TRMM Front Panel

Precautionary Procedures

Electrostatic discharge (ESD) can damage the static-sensitive devices on circuit boards. To avoid this kind of damage, use the following precautions when handling the TRMM:

- Do not remove the board from its antistatic shielding bag until you are ready to insert it into the hub.
- Use proper grounding techniques when inspecting and installing the TRMM. These techniques include using a foot strap and grounded mat or wearing a grounded static discharge wrist strap. An alternate method is to touch a grounded rack or other source of ground *before* you handle the TRMM.

Unpacking Procedure

To unpack the TRMM:

1. Verify that the TRMM is the correct model by matching the part number listed on the side of the shipping carton to the part number you ordered.
   - The part number of the Basic version is 43G3949.
   - The part number of the Advanced version is 43G3884.
2. Remove the module, in its antistatic bag, from the shipping carton.
3. Remove the module from the antistatic shielding bag and inspect it for damage. Always handle the module by the faceplate, being careful not to touch the components.

   If the module appears to be damaged, replace it in the antistatic shielding bag, return it to the shipping carton, and contact your local supplier.

IBM suggests you keep the shipping carton and antistatic shielding bag in which your module was shipped in case you later want to repackage the module for storage or shipment.

IBM also suggests that you record the serial number of your TRMM. A log for this and other information specific to your module is provided under the Slot Usage Chart in Appendix B of the *8250 Multiprotocol Intelligent Hub Installation and Operation Guide*.

Verifying Jumper Settings

The TRMM has three on-board jumpers, JP1, JP4 and, JP5. Jumpers JP1 and JP5 do not have their pins capped. Jumper JP4 has two of its three pins capped depending on the number of Flash EPROMs installed:

- Pins 1 and 2 are capped if eight Flash EPROMs are installed.
- Pins 2 and 3 are capped if four Flash EPROMs are installed.

This jumper setting *should not be changed*. Information on this jumper is included so that you can restore it to the proper setting if necessary.

Figure 3-1 shows the location of the jumper pins on the TRMM and their default settings. This figure illustrates jumper JP4 set for a board that has four Flash EPROMs installed.

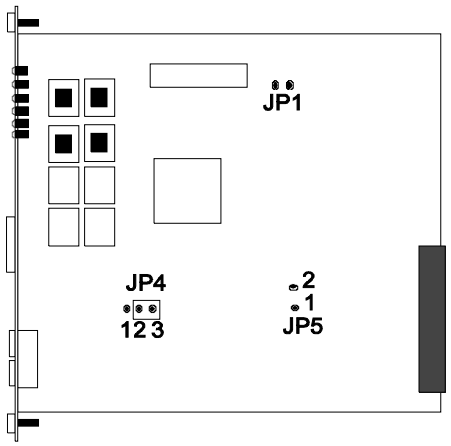


Figure 3-1. TRMM Jumpers and Default Jumper Settings

Advanced Board Installation

If you are installing the TRMM Advanced module (Feature Code 3884) or upgrading your TRMM Basic module to an Advanced module, you must first attach the Advanced board onto the Basic board as described in the steps below and illustrated in Figure 3-2.

1. Using a Phillips-head screwdriver, remove the three screws from the metal standoffs on the component side of the Basic board.
2. Connect the Advanced board connector to the Basic board connector.
3. To secure the Advanced board, re-install the three screws back into each of the three metal standoffs on the TRMM. Once the Advanced board is attached, complete the installation by following the procedures in the next section.

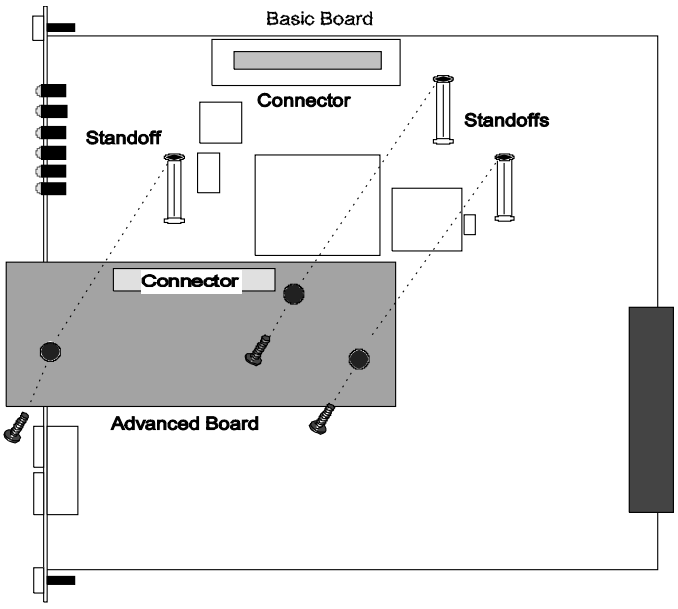


Figure 3-2. Attaching the Advanced Board to the Basic Board

Installing the Module

Installing the Token Ring Management Module into an existing installation *does not* require you to power down the hub. The TRMM, as with all other 8250 modules, has the ability to be "hot swapped." You can install the module into any open slot, and remove it while the hub is operating.

When you first install a new 8250 Multiprotocol Intelligent Hub and modules, the following steps must be performed *prior* to installing the TRMM:

1. Install the hub in its location (rack, table, and so on), referring to the instructions in the *8250 Multiprotocol Intelligent Hub Installation and Operation Guide.*

2. Install the Controller Module and all media modules into the board guides at the top *and* bottom of the slots and slide them into the hub.

3. Using your fingers, fasten the spring-loaded screws on the front panels of the modules to the hub (do not overtighten).

4. Plug the power cord into an outlet.

To install a TRMM into an 8250 Multiprotocol Intelligent Hub:

1. Install the TRMM into the board guides at the top *and* bottom of an empty slot and slide it into the hub as shown in Figure 3-3. Make sure the connector is firmly seated in the backplane of the hub.

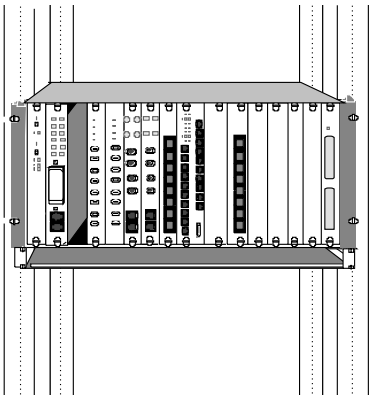


Figure 3-3. Installing the Token Ring Management Module

2. Using your fingers, fasten the spring-loaded screws on the TRMM faceplate to the hub (do not overtighten).

Wait for the following:

- Status LED lights solid green.
- BAS or ADV LED lights to indicate the TRMM version (Basic or Advanced).
- Master Mgt LED or the Backup LED lights to indicate whether the TRMM is configured as master or slave.

3. If you want to use a terminal (out-of-band) connection, verify that the terminal meets the factory defaults of the TRMM, or you will not be able to communicate with the module. The default TRMM settings are:
   - 9600 baud
   - 8 data bits
   - No parity
   - 1 stop bit
   - Enable XOFF/XON
4. Attach one end of an RS-232 cable to the RS-232 serial port connector on the front of the TRMM. Loop the cable through the hub cable tray (if installed) and attach the other end to the RS-232 serial port connector to a terminal or personal computer as shown in Figure 3-4.

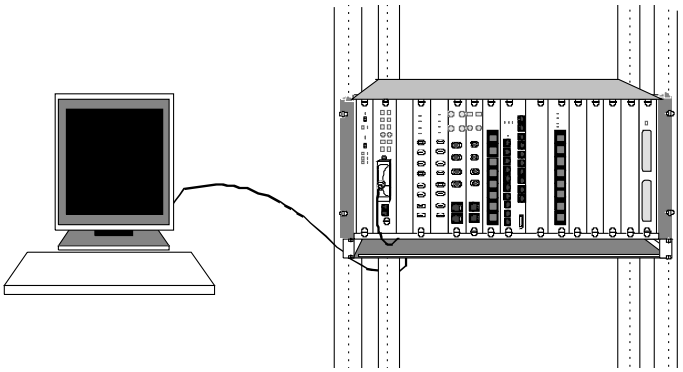


Figure 3-4. TRMM RS-232 Port Connected to a Terminal

The maximum recommended length for an RS-232 cable is 50 feet. There are several valid RS-232 cable configurations available depending on your installation. Refer to RS-232 Cable Specifications on page 3-19 for more information on the exact RS-232 cable that you need for your installation and for the correct pinouts.

5. Install the cables to the copper Ring-In and Ring-Out ports (if necessary). These ports are described in the following section.

Connecting Copper Ring-In/Ring-Out Ports

The primary purpose for the copper Ring-In and Ring-Out ports is for interconnecting the TRMM to either an 8250 Token Ring MAU Module in a hub or to a standalone MAU such as the IBM 8228.

Note: Cable Monitor mode must be disabled when connecting the TRMM to another hub or to a non-IBM device. Use the SET TRUNK RING_IN/RING_OUT CABLE_MONITOR command to enable or disable Cable Monitor mode.

Warning: Do not connect a TRMM and a 3822TR module using both the copper Ring-In/Ring-Out trunks and the backplane simultaneously. This is an invalid configuration and will segment the ring into two distinct rings.

Connecting to Trunks in the Same Hub

To connect the TRMM to a MAU Module in the same hub:

1. Attach one end of the twisted pair cable (STP-type only) to the copper Ring-Out port on the front of the TRMM.
2. Attach the other end to the copper Ring-In port on the MAU Module.
3. Interconnect any remaining MAU Modules using each module's Ring-In/Ring-Out ports. Be sure to make connections using both the copper Ring-In and Ring-Out ports to form a full ring. Also, you should use the IBM 43G3873 or 43G3874 cables for maximum fault tolerance between the TRMM and MAU Modules.

Figure 3-5 shows a TRMM connected to two 8250 Token Ring MAU modules.

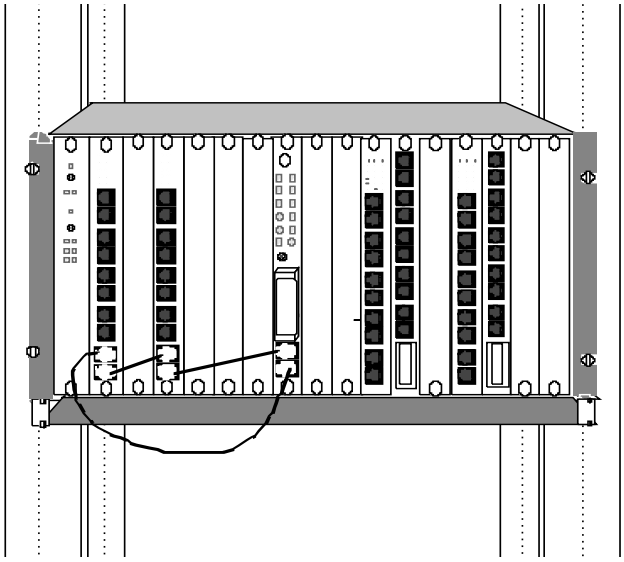


Figure 3-5. TRMM Connected to Two 8250 Token Ring MAU Modules

Connecting to External Trunks

To provide maximum fault tolerance for configurations that use multivendor equipment, the local ring should always start and end with the TRMM's copper Ring-In and Ring-Out ports. To connect to trunks external to the hub containing the TRMM:

1. Attach one end of the twisted pair cable (STP-type only) to the copper Ring-Out port on the front of the TRMM.
2. Attach the other end to the copper Ring-In port on a second 8250 hub or non-8250 device.
3. Issue the SET TRUNK *slot* RING_IN EXTERNAL_BEACON_ RECOVERY ENABLE command and the SET TRUNK *slot* RING_OUT EXTERNAL_BEACON_ RECOVERY ENABLE command to provide beacon recovery for the ring.
4. Issue the SET TRUNK *slot* RING_IN CABLE_MONITOR DISABLE command and the SET TRUNK *slot* RING_OUT CABLE_MONITOR DISABLE command to disable Cable Monitor mode.
5. Issue the SET TRUNK *slot* RING_IN NETWORK_MAP EXTERNAL command to ensure that the TRMM provides correct information when you issue the SHOW NETWORK_MAP command.

The configuration illustrated in Figure 3-6 shows how the copper ports are used to connect the TRMM to two IBM 8228 MAUs.

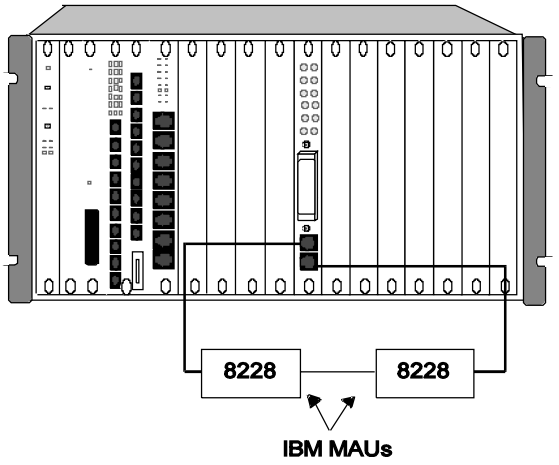


Figure 3-6. TRMM Connected to External MAUs

Verifying Operation

To verify the TRMM's functionality before you enter commands:

- The Status LED on the module should light. The Master Mgt LED should light if this TRMM is master.
- The BAS or ADV LED should light depending on whether the Basic or Advanced version of the TRMM is installed.
- The following message should display on the terminal screen once the module is installed properly and the RS-232 connection is made:

```
8250 Token Ring Management Module (vx.xx-A or B)
Copyright (c) 199x IBM Corporation.
```

See Chapter 4 for instructions on how to log in to the TRMM.

TRMM Front Panel

The TRMM has the following front-panel features:

- 12 module status LEDs
- Reset button
- Ring-In and Ring-Out ports
- RS-232 serial port connector

Figure 3-7 shows the features of the TRMM faceplate and Table 3-1 describes the LEDs.

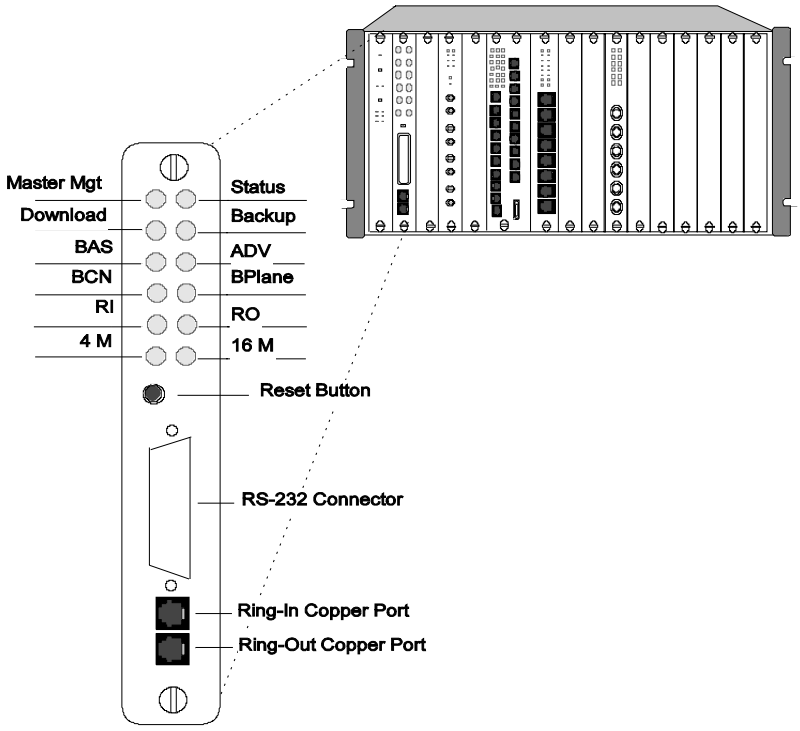


Figure 3-7. Token Ring Management Module Front Panel

Table 3-1. Interpreting the TRMM LEDs

LED Name	Color	State	Indicates
Master Mgt	Green	OFF	TRMM is a slave.
		On	TRMM is a master.
		Blinking	Mastership election is in progress.
Status	Green	OFF	Power off or complete failure.
		ON	Power on and software functioning properly.
Download	Yellow	OFF	Not downloading.
		On	Download of new software in progress.
Backup	Green	OFF	TRMM is master.
		On	TRMM is a slave.
BAS (Basic)	Green	OFF	Indicates Advanced TRMM.
		On	Indicates Basic TRMM.
ADV (Advanced)	Green	OFF	Indicates Basic TRMM.
		On	Indicates Advanced TRMM.
BCN (Beaconing)	Yellow	OFF	No beaconing present on the network.
		On	Beaconing present on the network.

Table 3-1. Interpreting the TRMM LEDs (Continued)

LED Name	Color	State	Indicates
BPlane (Backplane)	Green	OFF	Module is isolated from the backplane.
		On	Module is operating on the backplane.
RI (Ring-In)	Green	OFF	Port disabled.
		On	Port enabled and functioning properly.
		1 Blink	Ring-In port is wrapped due to no cable detected.
		2 Blinks	Port is wrapped because no signal is detected.
RO (Ring-Out)	Green	OFF	Port disabled.
		On	Port enabled and functioning properly.
		1 Blink	Ring-Out port is wrapped due to no cable detected.
		2 Blinks	Port is wrapped because no signal is detected.
4 M	Green	OFF	Indicates 16 Mbps ring speed.
		On	Indicates 4 Mbps ring speed. Ring operating properly.
		1 Blink	Ring set to 4 Mbps but TRMM cannot lock to signal.

Table 3-1. Interpreting the TRMM LEDs (Continued)

LED Name	Color	State	Indicates
16 M	Green	OFF	Indicates 4 Mbps ring speed.
		On	Indicates 16 Mbps ring speed. Ring operating properly.
		1 Blink	Ring set to 16 Mbps but TRMM cannot lock to signal.

Reset Button

The Reset button resets the TRMM and executes self-test diagnostics (network traffic is not affected). You should press this button *only* when you suspect problems with the TRMM. The Reset button is recessed to prevent an accidental reset, but can be pressed with a pen tip or a small screwdriver.

When the TRMM is reset, it will come up under the last saved configuration parameters. Therefore, it is important for you to issue the SAVE ALL command prior to resetting the module. Pushing this button has the same effect as issuing the RESET DEVICE command.

RS-232 Serial Port

The 25-pin (DB-25) RS-232 serial port is a DTE male connector used to connect the TRMM to a terminal or modem so you can enter management commands and download new software.

RS-232 Cable Specifications

The RS-232 cable connects to the management interface on the TRMM front panel. The management interface is designed to connect to a cable offering a female DTE interface. Table 3-2 defines the pinouts for an RS-232 cable for connecting devices to the management interface.

Table 3-2. RS-232 Cable Guidelines

Device	Connector (from terminal to TRMM)
Terminal	Female-to-female crossover (pin 2 to 3 and pin 3 to 2) Female-to-male crossover (pin 2 to 3 and pin 3 to 2)
Modem	Female-to-male straight-through (1 to 1, 2 to 2, ...)
Terminal Server	Refer to supplier documentation

When you first connect your terminal to the TRMM management interface, make sure the terminal is properly set for asynchronous serial communication. Figure 3-8 illustrates the RS-232 connector on the TRMM front panel and shows the proper pinouts for a crossover RS-232 cable.

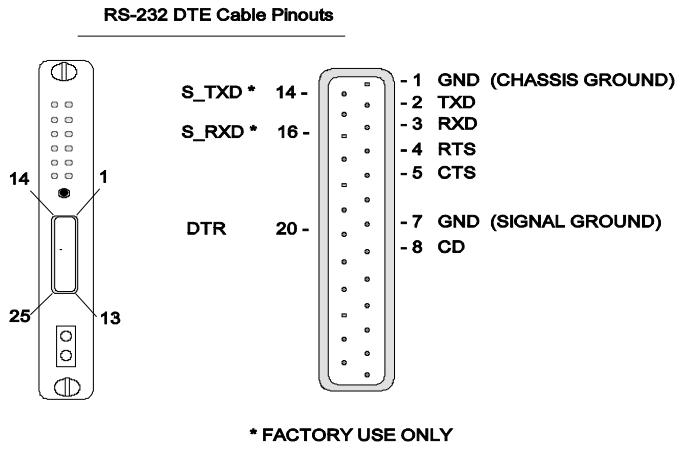


Figure 3-8. TRMM RS-232 Connector Pinouts

Modem Use

The Token Ring Management Module permits dial-in modem usage. The requirements are as follows:

1. The modem must be 100% Hayes** compatible.
2. Any baud rate in the range (300, 1200, 2400, 9600) may be used. Higher rates provide faster performance.
3. The modem must be placed in Dumb/Auto Answer mode by entering the following commands from a terminal directly connected to the modem:

a	**at&F**	**Enter**	Restore factory defaults
*b	**at&d0**	**Enter**	Ignore changes in DTR status
c	**ats0=1**	**Enter**	Auto-answer on first ring
d	**ats0?**	**Enter**	Verify auto-answer (should return 001)
e	**atq1**	**Enter**	Does not return result codes
f	**at&W**	**Enter**	Save this configuration
g	**at&Y**	**Enter**	Define this configuration as default
h	**ate0**	**Enter**	Cancel echo mode

***** If you issue the SET TERMINAL HANGUP ENABLE command for modem use, you must change the DTR parameter as follows to ensure proper modem operation:

*I	**at&d2**	**Enter**	Indicates hangup and assumes command state when an ON to OFF transition of DTR occurs

Chapter 4. Preparing the TRMM Command Interface

This chapter describes how to configure the TRMM once you have completed the installation procedures outlined in Chapter 3. Included in this chapter is a quick reference chart for getting started. The remainder of the chapter contains the following sections:

- Quick Reference for Getting Started
- Configuring the Terminal
- Configuring the TRMM
- Configuring User Logins
- Setting SNMP Values
- Using TELNET for Remote Logins

The commands necessary to configure the TRMM for operation are provided in this chapter. Refer to the *8250 Management Commands Guide* (Document Number SA33-0302) for complete information on all 8250 management commands and conventions.

Quick Reference for Getting Started

Table 4-1 outlines the steps necessary to configure your TRMM. The procedures and command examples are explained further throughout this chapter. If you are familiar with these instructions, you may want to use this table as a checklist.

Table 4-1. Quick Reference for Getting Started

Procedure	Command
1. Configure your terminal to default TRMM communication settings	Refer to your terminal vendor's documentation
• Configure TRMM terminal settings	SET TERMINAL CONSOLE HANGUP SET TERMINAL PROMPT SET TERMINAL TIMEOUT
2. Configure the TRMM	
• Concentrator Configuration	SET CONCENTRATOR PLATFORM SET CLOCK
• Device Configuration (TRMM)	SET DEVICE CONTACT SET DEVICE DIAGNOSTICS SET DEVICE LOCATION SET DEVICE NAME SET LOGIN
3. SNMP Configuration	SET COMMUNITY SET DEVICE DEFAULT_GATEWAY PRIMARY/SECONDARY SET DEVICE IP_ADDRESS SET DEVICE SUBNET_MASK SET ALERT SET DEVICE TRAP_RECEIVE

Table 4-1. Quick Reference for Getting Started (Continued)

Procedure	Command
4. Module Configuration	SET MODULE MASTERSHIP_PRIORITY SET MODULE NETWORK SET MODULE RING_SPEED
5. Port Configuration	SET PORT SET PORT MODE SET PORT STATION_TYPE SET SECURITY PORT
6. Save All Configuration Values	SAVE ALL

Saving and Reverting Configuration Values

When you make configuration changes using the SET command, they are effective immediately (except for MAC address, IP address, subnet mask, and default gateway) but are not saved permanently. To save settings permanently, issue the SAVE command. Only *saved* values are in effect upon reset of the TRMM or the hub.

Note: The SAVE ALL and SAVE MODULE_PORT commands automatically save all module and port configuration parameters to any slave TRMMs in the hub.

You can issue the SAVE ALL command to save all current hub configuration values previously established by the SET command for all categories. Or, you can issue a specific SAVE command to save the configuration values of only one group.

Use the REVERT command to restore the configuration values in effect at the time of the last save. Any unsaved changes made using the SET

command are lost. You can issue the REVERT ALL command to revert all current hub configuration values previously established by the SET command for all categories. Or, you can issue a specific REVERT command to revert the configuration values of only one group.

The SAVE and REVERT commands support the following configuration groups:

- Alert
- All
- BootP
- Community
- Concentrator
- Device
- Group
- Module_Port
- Schedule
- Scripts
- Security
- Terminal
- TFTP
- Threshold

Configuring the Terminal

The terminal that attaches to the serial port on the TRMM must be configured to the same parameter settings as the TRMM so the terminal and TRMM can communicate. These settings include:

- baud rate
- data bits
- parity
- stop bits

Initially, the terminal settings must match the factory default settings of the TRMM as specified in Table 4-2. Consult the user's guide shipped with your computer terminal for instructions on how to set the terminal values.

Table 4-2. TRMM Terminal Defaults and Commands

Parameter	Options	Factory Default
Baud	300, 1200, 2400, 4800, 9600	9600
Data_bits	7 or 8	8
Parity	odd, even, or none	none
Stop_bits	1 or 2	1

Logging in for the First Time

Once you have configured your terminal to match the factory defaults of the TRMM:

1. Press Enter. The following message is displayed:

```
Token Ring Management Module (T01MS-MGTx) vx.xx
Copyright (c) 1996 IBM Corporation


Login:
```

2. Type `system`, which is the default super-user login, then press Enter. The TRMM prompts you for a password:

   - If you are upgrading from TRMM Version v3.3 or earlier, enter your administrator password.
   - If this is a new TRMM installation, the default password is to press Enter.

3. Press Enter again. The following greeting and management prompt are displayed:

```
Welcome to super user service on 8250.
8250>
```

You are now logged in as the administrator with full access to all commands. Once terminal settings are complete, you can configure the 8250 Multiprotocol Intelligent Hub, the newly installed TRMM, and all other 8250 modules residing in the hub.

When you are done using the TRMM, save all changes, and then log out of the system using the LOGOUT command. Provided you have saved all changes before issuing this command, you are logged out of the system and the following message displays:

```
8250> logout
Bye
```

If you have made configuration changes and you have not saved those changes, the LOGOUT command prompts you as follows:

```
8250> logout
WARNING: Save unsaved changes before logout.
```

You must either save or revert any changes you made to the system before you can log out. Once you have saved or reverted changes, re-issue the LOGOUT command to log out of the system.

Optional Terminal Settings

The TRMM provides three additional terminal management commands you can use to customize your terminal connection:

- SET TERMINAL HANGUP
- SET TERMINAL PROMPT
- SET TERMINAL TIMEOUT

These terminal settings are discussed in the following sections.

Setting Terminal Hangup

If you use a modem connection to the TRMM, you may want to have the modem automatically hang up the connection to the terminal when you log out of the TRMM. The factory-default setting is disable, which means the modem will *not* automatically hang up when you log out of the connection.

Use the SET TERMINAL CONSOLE HANGUP command to hang up the modem connection automatically once you log out of the TRMM:

```
8250> set terminal console hangup enable
```

Note: If you fail to hang up the modem connection, an unauthorized user may pick up the last login session.

Setting the Terminal Prompt

It is a good idea to customize the terminal prompt for each TRMM. This reminds you of the TRMM to which you are connected when you are logged in to a remote TRMM. The default terminal prompt for all TRMMs is 8250>. Use the SET TERMINAL PROMPT command to customize your terminal prompt:

```
8250> set terminal prompt TRMM4>
TRMM4>
```

Note: IBM recommends that you use the same identification to specify both the terminal prompt and the device name for your TRMM.

Setting Terminal Timeout

For optimum security control, set the terminal timeout value to specify the amount of time you want your terminal to remain active during the absence of any keyboard activity. This feature is useful for preventing unauthorized users from gaining access to the system if you leave your terminal without logging out. Once timeout has been set, the terminal automatically logs you out of the system if there is no terminal (keyboard) activity for the period of time you have specified.

The default timeout value is 0, which means that no timeout has been set; you will never be logged out automatically. Use the SET TERMINAL TIMEOUT command to set the timeout period. Note that the value specified is in minutes.

```
8250> set terminal timeout 10
```

Configuring the TRMM

This section describes the commands necessary for startup and management of your hub and TRMM. The TRMM is factory-set to default values that you may need to change before using it (for example, the mastership priority of the TRMM). You must be logged in under the super user password in order to change these values.

You need to define the following settings for your TRMM:

- Platform Type
- TRMM Name
- Diagnostics
- TRMM Clock
- Contact Name and Location
- Mastership Priority

Setting Hub Platform

Use the following command to define the type of hub in which the TRMM resides as a 17-slot hub.

```
8250> set concentrator platform 8250-017
```

Note: Use the 8250-006 designation for all 6-slot hubs.

Setting the Internal Clock

Use the SET CLOCK command to establish a starting time, date, and day. This setting needs to be defined only once, at the time you install the TRMM into your hub. The following example shows you how to set the 24-hour internal clock to *5:53PM, Sunday, March 10th, 1996.*

```
8250> set clock 17:53 96/03/10 sunday
```

The internal clock is powered by its own battery and continues to work even when the hub loses power. This battery is designed to operate for 10 years.

Assigning TRMM Names

To make identification of your TRMMs easier, assign a unique name to each TRMM. You can use this name instead of the IP address or the MAC address to refer to a particular TRMM. Use the same identification to specify the terminal prompt and the device name for your TRMM.

Use the SET DEVICE NAME command to assign a unique name to your TRMM. The TRMM name can be a maximum of 31 characters long.

```
8250> set device name TRMM3
```

Assigning Contact Names and Locations

The TRMM enables you to enter the name of a service contact and hub location. Use the SET DEVICE LOCATION and SET DEVICE CONTACT commands to identify the name of the person responsible for the TRMM and the location of the TRMM.

These commands allow you to enter one line of free-format text up to 78 alphanumeric characters in length. You must enter the line of text within 15 seconds of receiving the prompt or the command times out.

```
8250> set device location
> Bld.1 Floor 3 Eng Wiring Closet
8250> set device contact
> System Administrator
```

Setting Device Diagnostics

When the TRMM is reset (or rebooted) using the factory-default settings, the module performs a full diagnostic self-test and then sets all of the modules to the appropriate settings.

You can disable diagnostics if you want the TRMM to boot faster. Use the SET DEVICE DIAGNOSTICS command to bypass the diagnostics.

```
8250> set device diagnostics disable
```

Assigning Module Mastership Priority

All 8250 management modules are shipped from the factory with a mastership priority level of 10, the highest priority. When multiple management modules reside in the same hub, the SET MODULE MASTERSHIP_PRIORITY command enables you to establish one of the modules as the master management module and all other modules as slaves.

A TRMM master provides beacon recovery and manages the network to which it is assigned, controls all configuration, and supplies all fault-detection capabilities for the entire hub. A slave management module can only listen to its assigned network's activity. Both master and slaves can collect statistics on *only* one network at a time. The first TRMM you place in a hub should maintain the default mastership priority level of 10. Once installed, the priority levels of all other TRMMs should be changed to mastership priority level 1 (slave).

Use the following command to set the module in slot 7 to mastership priority level 1.

```
8250> set module 7 mastership_priority 1
```

Once mastership priorities are assigned, you must issue the RESET MASTERSHIP command to initiate an election. During an election, the management module with the highest assigned mastership priority becomes the master. The new mastership setting is in effect immediately, but you must use the SAVE MODULE_PORT command to save this priority permanently.

Note: When you power up a hub in which more than one management module is set to priority level 10, one management module is randomly chosen as master. IBM recommends that you assign priority level 10 to only one management module in the hub. Any other management modules in the same hub should then be set to priority level 1.

Configuring User Logins

This section describes:

- User Access Levels
- User Login Functions
- Adding New Users
- Showing Current Users
- Clearing Login Names

Warning: Refer to Logging in for the First Time on page 4-5 when you log into TRMM Version v4.0 or later for the first time.

User Access Levels

TRMM provides three levels of user access:

- **User Level** — Allows the user to display information about network configuration and operation (except community table information).
- **Administrator Level** — Allows the user to perform all user-level tasks, as well as:
  - Reset and configure 8250 modules and ports (SET commands)
- **Super User Level** — Allows the user to perform administrator- and user-level tasks, enter maintenance mode, and add and change passwords, as well as:
  - Configure hub IP address information
  - Configure community tables
  - Download new flash and boot code

User Login Functions

TRMM allows:

- Configuration of up to 10 user logins, in any combination of access levels
- More than one user at a time to log in to the command interface

The only configuration limitation is that only one user at a time can log in with write privileges. If a second administrator or super user tries to log in, that user has access to user-level (read) functions only. Up to four remote (TELNET) sessions can be established at one time.

Because the TRMM only allows one super user login at a time, the software includes a special SET LOGIN ACCESS SUPER_USER command. If a super user logs in and is granted only user privileges, that user can issue the SET LOGIN ACCESS SUPER_USER command with the following results:

- The current super user is logged off the TRMM
- The super user issuing the command immediately assumes super user privileges
- The new super user assumes responsibility for all unsaved changes from the logged-out super user session

This command can also be used to override sessions in which communications have failed but the super user remains logged in. Without this command, you must wait for the disrupted super user session to time out before you can initiate a new super user session.

Adding New Users (Requires Super User Authority)

As stated in the previous section, the TRMM allows you to configure up to 10 user logins, with access rights as described above.

To configure a new user:

Note: To add login names, you must be logged in using a user name that has been assigned super user privileges.

1. Log in using a super user-level name and password.
2. At the prompt, enter SET LOGIN *login type*, then press Enter. The system prompts for your password (to confirm your right to set new passwords) as follows:

   ```
   Enter current session password for user "system":{enter
   password}
   ```

3. At the `Enter Login Name:` prompt, enter the login name for the user you want to add.
4. At the `Enter Login Password:` prompt, enter the login password.
5. At the `Verify - re-enter password:` prompt, retype the new password.
6. Enter the SAVE LOGIN command to save the new user login.

The system acknowledges the new password by displaying:

```
Login successfully entered.
```

Showing Current Users

To show the existing login names for the TRMM, enter the SHOW LOGIN command. The following displays:

```
Index   Login Name       Access          Active Sessions
-----   --------------   -------------   ---------------
    1   system           Super User           1
    2   kwillow          User                 0
    3   test1            User                 0
    4   [not used]
    5   [not used]
    6   [not used]
    7   [not used]
    8   [not used]
    9   [not used]
   10   [not used]

Active Login Sessions:

     Login Name       Session Type              Session Time
     ----------       ------------              ------------
     system           Remote Super User         0 days 00:08:05
     system           Remote User               1 days 01:08:06
```

Table 4-3 describes the fields in the SHOW LOGIN display.

Table 4-3. SHOW LOGIN Display Fields

Column	Description
Index	Index number of each of the 10 available logins
Login Name	The name assigned to each login (or [not used])
Access	Privilege level assigned to this login name (refer to User Access Levels on page 4-12)
Active Sessions	Number of active sessions under this login name
Active Login Sessions	**Session Type** — Indicates user privileges and whether session is local or remote **Session Time** — Length of the session

Clearing Login Names

You may want to clear login names from the TRMM periodically to help ensure system security. To clear a login name from the TRMM:

1. Enter CLEAR LOGIN *index number*

   or

   CLEAR LOGIN ALL to clear all logins not currently logged in with Active Sessions.

2. Press Enter.

If you are not sure of the index number for the user name you want to clear, enter SHOW LOGIN for a list of all login names (and corresponding index numbers) available for this TRMM.

Setting SNMP Values

SNMP (Simple Network Management Protocol) is a protocol defined by the Internet community. SNMP is encapsulated in a UDP and IP packet, which in turn is encapsulated in a Token Ring 802.5 frame.

The TRMM supports SNMP by responding to SNMP requests and generating SNMP traps. A TRMM acts as an agent in an SNMP-managed environment, enabling you to configure your TRMM, and all modules in the hub, through SNMP. The TRMM has a community table that can contain up to 10 IP addresses.

An IP address entry in a community table may have one of the following attributes assigned:

- **read-only** allows the specified IP address to read SNMP variables using the SNMP GET command.
- **read-write** allows the specified IP address to read and write SNMP variables using the SNMP GET and SNMP SET commands, respectively.
- **trap** sends a trap to the specified IP address when an SNMP variable is changed.
- **read-trap** allows the specified IP address to read SNMP variables and receive traps.
- **all** (read-write and trap) allows the specified IP address to read SNMP variables, change the variables using the SNMP SET command, and receive traps whenever an SNMP variable is changed.

You must assign community privileges to a management station IP address as follows:

- To receive traps, assign trap, read-trap, or all
- To allow TRMM configuration using SNMP, assign read-write or all
- To monitor the TRMM, assign read-only, read-write, read-trap, or all

Receiving SNMP Alarms

A TRMM can receive SNMP alarms from SNMP devices on the network (including itself). The TRMM receives SNMP alarms if its IP address and accompanying attributes have been added to the community table of the SNMP device generating the alarms, and the SET ALERT feature is enabled.

For example, if a major fault condition causes a port to beacon, an SNMP trap is generated and displays to the terminal or workstation. This feature enables you to analyze network information by accessing a single TRMM instead of having to be at the network management workstation.

If you plan to manage your hub through an SNMP workstation, you must set the following attributes for the TRMM:

- IP Address
- Alerts
- Default Gateway
- MAC Address Type
- Community Table
- Subnetwork Mask
- Trap Receive

Assigning IP Addresses

To run SNMP, every device on your network must have a unique IP address. Use the SET DEVICE IP_ADDRESS command to assign an IP address to the TRMM on a Token Ring network. You can set separate IP addresses for each of the individual networks on the hub backplane.

The following example assigns IP address 195.36.58.27 to the TRMM on Token Ring network 3:

```
8250> set device ip_address 195.36.58.27 token_ring_3
```

Once you change the IP address, connection to the old IP address is lost. Therefore, you must reset the TRMM and re-establish the connection.

Creating a Community Table

The community table defines which SNMP stations on the network can access information from the TRMM, and which stations receive a trap from the TRMM when the TRMM detects an error.

Use the SET COMMUNITY command to create a community table entry. The following example adds a community name of NCS with IP address 195.36.58.217 to have read_write access:

```
8250> set community NCS 195.36.58.217 read_write
```

Note: Community entry names are case-sensitive. For example *NCS* and *ncs* are *different* community names.

Use the SHOW COMMUNITY command to view existing community entries.

Configuring the Alert Setting

Use the SET ALERT command to enable or disable the feature for sending an alert to the management workstation. The following command enables the alert feature. When a configuration change is made to the hub using SNMP, an alert is sent to the management workstation.

```
8250> set alert change enable
```

Refer to the description of the SET ALERT command in the *8250 Management Commands Guide* for information on the different types of alerts available through this command.

Setting a Subnetwork Mask

The subnetwork mask is specific to each type of Internet class. Generally, the subnetwork mask is a group of common characters appearing on the left side of an IP address (called the Network ID), while the host address is the group of unique characters appearing on the right side of an

IP address. For example, to set the subnetwork mask for a class C address without subnetworks, enter the following command:

```
8250> set device subnet_mask FF.FF.FF.00 all
```

The subnetwork mask for a class B device, without subnetworks, would be set using the following command:

```
8250> set device subnet_mask FF.FF.0.0 token_ring_3
```

Note that you can set separate subnetwork masks for each of the individual networks on the hub backplane, or the same subnetwork mask for all of the networks on the hub backplane.

Defining the Default Gateway

The default gateway is the IP address of the gateway that receives and forwards packets whose addresses are unknown to the local network. The default gateway is useful when sending TRMM alert packets to a management workstation on a different network. You can set separate default gateways for each of the individual networks on the hub backplane, or the same default gateway for all of the networks on the hub backplane. In addition, the TRMM enables you to define both a *primary* and *secondary* default gateway.

The following command defines IP address 195.3.6.58 as the primary default gateway for all Token Ring networks:

```
8250> set device default_gateway 195.3.6.58 all primary
```

The following command defines the IP address 128.3.6.3 as the secondary default gateway for all Token Ring networks:

```
8250> set device default_gateway 128.3.6.3 all secondary
```

The secondary default gateway feature detects if the gateway that the TRMM is using is no longer available. If the primary default gateway becomes unavailable, the TRMM switches from the current default gateway to the secondary default gateway.

To detect a malfunctioning gateway (and not produce excessive network traffic), the TRMM verifies that the gateway is active when it needs to

communicate with it. If no packets have been received from the gateway MAC address, every 30 seconds the TRMM forces an ARP (Address Resolution Protocol) request to the gateway when the TRMM needs to communicate with it. If no ARP response is received after two requests, the gateway is considered to be malfunctioning.

When the TRMM detects a malfunctioning gateway, it sends an ARP request to the other entry (primary or secondary). If the TRMM receives a response, it sets the default gateway to that entry. The TRMM will always attempt to use the primary gateway as the default gateway upon a reset.

The SHOW DEVICE display contains both primary and secondary gateway fields. The active gateway is indicated by a pound sign (#).

Enabling Trap Receive

You can define the TRMM as a trap receiver. As a trap receiver, the TRMM receives traps from other SNMP devices that have the TRMM IP address in their community table.

Use the following command to enable a TRMM to function as the trap receiver for other SNMP devices on the network:

```
8250> set device trap_receive enable
```

Note: You must add the TRMM IP address to a device community table for that device to be able to send traps to the TRMM.

Defining MAC Address Type

The local administration of the TRMM MAC address enables you to specify the TRMM MAC address as either the factory-default MAC address (burned_in) or user-defined (locally_administered).

Use the following command to specify the locally administered MAC address in slot 7:

```
8250> set module 7 locally_administered_address 40-10-50-10-23-33
```

The TRMM rejects this command if the MAC address specified as the TRMM MAC address is 0-0-0-0-0-0. Bit 2 of the locally administered MAC address must be a 1. In the above MAC address example, bit 2 is 1, which is indicated by 4 in the first hexadecimal digit.

Use the following command to specify the MAC address as locally administered for the TRMM in slot 7:

```
8250> set module 7 mac_address_type locally_administered
```

Using TELNET for Remote Logins

The TELNET command enables you to log in remotely to any TRMM on the network, and to manage the network remotely (from a terminal attached to a remote TRMM, or from a workstation with TELNET support). You can manage a TRMM across any number of bridges and routers. Each TRMM supports up to four simultaneous incoming TELNET sessions.

You can also use the TRMM to connect to other devices by using the TELNET command to specify the IP address of the remote TRMM to which you want to connect. You must be logged in to the local hub before you can issue the command.

```
8250> telnet 127.3.6.58
```

Once you are connected to a remote TRMM, you must log in to that TRMM. Once logged in, all of the commands you issue are for that TRMM. Refer to the *8250 Management Commands Guide* for a complete description of the TELNET command.

As shown in Figure 4-1, if you are locally connected to the TRMM in Hub C, you can remotely log in and manage the TRMMs in Hubs A and B. Note that you are allowed only one outgoing TELNET login session for each TRMM. Therefore, it is not possible to use the TRMM in Hub C to log in to Hub A *and* Hub B simultaneously.

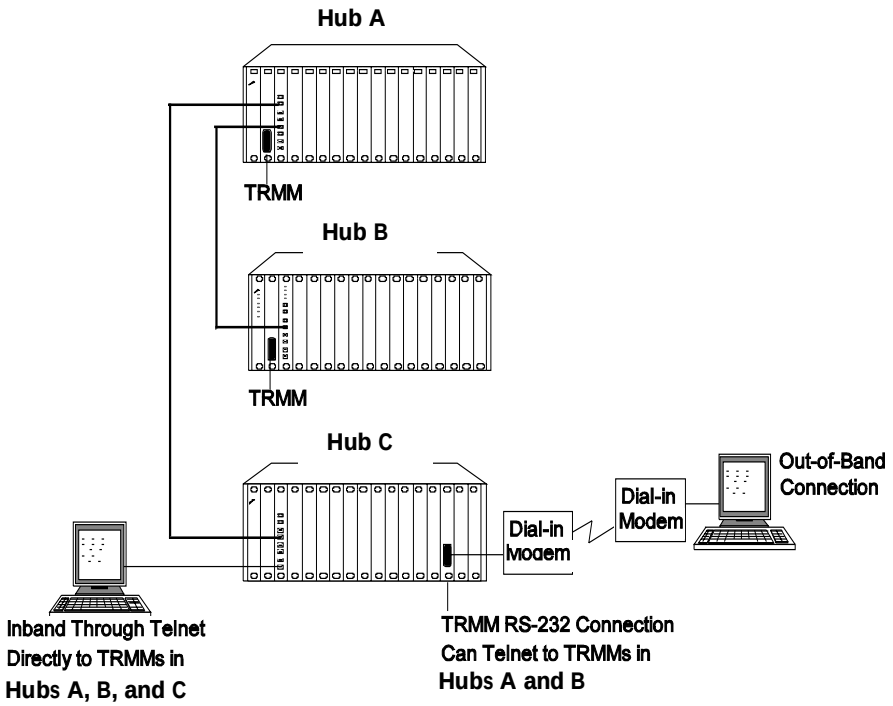


Figure 4-1. Sample Remote Connection

Logging Out From a Remote Session

When you no longer need to be connected to a remote device, enter the LOGOUT command. This command disconnects the remote connection and reconnects the session with the local TRMM. Once this is done, the local management prompt returns to the local screen and the system displays the message `Remote session completed`.

```
82502> logout
Bye
Remote session completed
8250>
```

Warning: If TIMEOUT has been set for the remote TRMM and the time runs out, you are logged out of the remote TRMM and returned to the local TRMM. Unsaved changes are still in effect, but they will be lost if the TRMM is reset. To save these changes, re-establish connection to the TRMM and issue the SAVE command.

Chapter 5. Using TRMM Features

This chapter describes TRMM features you can use to manage your Token Ring network. The chapter contains the following sections:

- Configuring Modules and Ports
- Configuring Address-to-Port Security
- Using Beacon Recovery Commands
- Using BootP
- Using Scheduling
- Using Scripting
- Using the TRMM Advanced Port Groups
- Using the TRMM Advanced Thresholds
- Configuring Fiber Trunk Redundancy
- Using the SHOW Commands

Configuring Modules and Ports

This section describes how to assign the TRMM and media modules to a backplane Token Ring network and how to configure your Token Ring ports correctly. This section contains the following subsections:

- Assigning Module Networks
- Assigning a Slave TRMM to a Network
- Defining Module Ring Speed
- Setting Port Mode
- Setting Port Station Type

Appendix B of the *8250 Multiprotocol Intelligent Hub Installation and Operation Guide* provides a chart to record the values you set for modules in your hub.

Assigning Module Networks

Modules assigned to the same network form a ring. Modules assigned to different networks are on different rings; these rings cannot communicate with each other unless the networks are bridged. All 8250 modules, except the Fault-Tolerant Controller Module and the Token Ring MAU Module, can be assigned to a network. The Controller Module does not require a network assignment because it connects to the control bus only. The MAU Module connects through its trunk or Ring-In/Ring-Out ports only.

If you isolate a module, the isolated module cannot send or receive any traffic from other modules in the hub. An isolated TRMM can receive traffic through the copper Ring-In/Ring-Out ports. Initially, all 8250 modules are factory-set to network 1, but come up isolated if a management module is installed in the hub.

For example, use the following command to assign the module in slot 7 to Token Ring network 3:

```
8250> set module 7 network token_ring_3
```

Note: When you switch Token Ring modules from one ring to another ring, the rings are momentarily joined. To avoid this situation, switch the modules to isolated before switching them to another ring. The momentary joining of the rings does not adversely affect the ring, nor does it have any effect on user applications.

Assigning a Slave TRMM to a Network

The TRMM enables you to define the network a slave TRMM will be assigned to in the event it becomes the master TRMM. For example, a master TRMM is configured for Token_Ring_1 and a slave TRMM is configured for Token_Ring_2. You can specify that the slave TRMM reconfigure to Token_Ring_1 in the event it becomes master TRMM.

For example, use the following command to define Token Ring 1 as the network assignment for the slave TRMM:

```
8250> set module 7 master_network token_ring_1
```

Defining Module Ring Speed

Token Ring modules must be configured to operate at a transmission rate of 4 Mbps or 16 Mbps to match the network's ring speed.

For example, use the following command to set the module in slot 7 to a 16 Mbps ring speed:

```
8250> set module 7 ring_speed 16mbps
```

Setting Port Mode

The SET PORT MODE command allows you to enable and disable media module ports in the hub.

For example, use the following command to enable port 1 on the module in slot 7:

```
8250> set port 7.1 mode enable
```

Setting Port Station Type

Stations that assert phantom current, but do not have a MAC address (for example, a network analyzer) may cause problems in the Token Ring mapping algorithm. To prevent this problem, use the SET PORT STATION_TYPE command to set the station type parameter to MAC_NOT_PRESENT. This setting eliminates a MAC-less station from the mapping algorithm.

For example, use the following command to define the station type of port 6 on the module in slot 3 as mac_not_present:

```
8250> set port 3.6 station_type mac_not_present
```

Configuring Address-to-Port Security

Address-to-port security allows you to assign up to four MAC addresses to each port in your network. When a TRMM detects a port MAC address that is not in the list assigned to this port, it disables the port to preserve network security, and sends a trap to any station configured in the TRMM community table to have trap or all access.

Once you correct the security violation (by either removing the station or adding its MAC address to the list), you must issue the SET PORT MODE ENABLE command to re-enable the port.

To implement port security you must assign a MAC address to a given port before you enable the security feature for that port.

For example, use the following command to assign a MAC address to port 6 on the module in slot 3:

```
8250> set security port 3.6 mac_address 08-00-8f-12-c0-09
```

Use the following command to enable the security feature for port 6 on the module in slot 3:

```
8250> set security port 3.6 mode enable
```

If you use the all option instead of specifying a slot and port, the TRMM sends the command to modules in the hub that support security.

Use the SHOW SECURITY PORT command to display the MAC address and security setting for a specific module and port, for all ports, or for all ports of a specific module.

The following example displays security settings for all ports on the module in slot 7:

```
8250> show security port 7.all

Security Display for Module T08MS-RJ45S:

Port    Mode      MAC Address        General Information
07.01   ENABLED   08.00.8f.1b.0b.ad  TOKEN_RING_1
07.02   ENABLED   08.00.8f.3c.c6.1e  TOKEN_RING_1
07.03   ENABLED   08.00.8f.00-0e-c6  TOKEN_RING_1
```

Using Beacon Recovery Commands

This section describes the following commands:

- Beacon Timeout Command
- Beacon Trunk Retry
- Trap Log

Beacon Timeout Command

The BEACON_TIMEOUT command enables you to define a time limit that the TRMM uses to keep a port disabled during beaconing. The time limit is based upon the timeout value. The default value is 10 seconds.

The syntax of the BEACON_TIMEOUT command is as follows:

```
set device beacon_timeout 1 to 100 seconds
```

Because the Beacon Timeout value is not stored in the permanent storage of the TRMM, you must reconfigure the value if the TRMM is reset.

To display the current Beacon Timeout value, use the SHOW DEVICE command. There is no SNMP support for the Beacon Timeout feature.

Beacon Trunk Retry Feature

The Beacon Trunk Retry feature:

- Allows you to configure the number of times the TRMM re-enables trunks disabled due to beaconing conditions.
- Eliminates the need for you to re-enable trunk configurations manually.

Beacon Recovery Algorithm

By default, the beacon recovery algorithm causes the TRMM to re-enable trunks that have been disabled during the beacon recovery process. After the TRMM has tried twice to re-enable trunks, one of the following conditions exists:

- Beaconing is resolved and trunks remain enabled.
- Beaconing is still present on the ring and trunks remain disabled.

If a trunk remains disabled after beacon recovery completes:

1. The TRMM checks the Beacon Trunk Retry value. If the value is greater than 0, the TRMM re-enables the trunk. If the beaconing condition is resolved, the trunk remains enabled and the TRMM does not perform any other beacon recovery actions.
2. If beaconing recurs as a result of the TRMM re-enabling the trunk, the TRMM re-enters the beacon recovery algorithm and decrements the Beacon Trunk Retry value by 1.
3. If the trunk remains disabled once the beacon recovery algorithm completes, the TRMM checks the Beacon Trunk Retry value. If the value is greater than 1, the TRMM re-enables the trunk until either one of the following conditions occurs:
    - The Beacon Trunk Retry value decrements to 0.
    - The trunk is enabled and beaconing is resolved.

The syntax for configuring a TRMM Beacon Trunk Retry value is as follows:

```
set device beacon_trunk_retry value (0 to 255)
```

Where:

- 1 to 254 (inclusive) allow the TRMM to terminate attempts to re-enable trunks once the number of retry attempts is reached or beaconing has been resolved.

- 255 specifies that the TRMM will attempt to re-enable trunks indefinitely until beaconing is resolved.

The default (and recommended) value for the Beacon Trunk Retry feature is 0.

For example, to configure the TRMM to re-enable trunks once, enter the following command:

```
8250>  set device beacon_trunk_retry 1
```

When a beaconing condition exists, the TRMM, by default, twice re-enables the trunks that were disabled due to beaconing. When the Beacon Trunk Retry value is set to 1, the following actions occur:

1. If the trunks remain disabled once the beaconing recovery algorithm completes, the TRMM checks the Beacon Trunk Retry value.

2. The TRMM re-enables the trunk once. If beaconing recurs as a result of the TRMM re-enabling the trunk, the TRMM re-enters the beacon recovery algorithm and decrements the Beacon Trunk Retry value to 0.

    - If beaconing is present, the trunks are disabled and no further beacon recovery actions are taken.

    - If beaconing is resolved, the trunks remain enabled and the TRMM stops trying to enable the trunks.

To save the Beacon Trunk Retry value, use the SAVE ALL or SAVE DEVICE command. The Beacon Trunk Retry setting is reported in the SHOW DEVICE command display. There is no SNMP support for this feature.

Trap Log

The Trap log is a log file that contains a maximum of 15 entries describing trap conditions. For beaconing conditions, the Trap log maintains entries for the following devices that are disabled or re-enabled due to beaconing:

- Modules
- Ports
- Trunks

To display the Trap log, enter the following command:

```
8250>  show log trap_log
————————-TRAP 1————————
Message received from this device on 10:22 Fri 24 May 96:
Enterprise:            IBM
Enterprise Specific trap:  Trunk Down
Message Information:
    Slot Number:      12
    Trunk Number:      3
    Trunk Mode:       DISABLED
    Trunk Status:     BEACONING
    Trunk Wrap State: WRAPPED
–More–
————————-TRAP 2————————
Message received from this device on 10:22 Fri 24 May 96:
Enterprise:            IBM
Enterprise Specific trap:  Trunk Down
Message Information:
    Slot Number:      12
    Trunk Number:      3
    Trunk Mode:       ENABLED
    Trunk Status:     BEACONING
    Trunk Wrap State: UNWRAPPED
```

To clear the Trap log, enter the following command:

```
8250> clear log trap_log
Trap log is cleared.
```

Using BootP

BootP (Bootstrap Protocol) is available on the TRMM. BootP is a UDP/IP-based protocol (User Datagram Protocol/Internet Protocol) that allows a device to configure itself dynamically without user intervention. Use BootP to download configuration information from the *bootptab* file on a server to the TRMM.

You need to maintain a bootptab file on the BootP server that contains:

- TRMM MAC address
- TRMM IP address
- Default gateway
- Subnet mask
- TFTP variables (such as file name, file type, and file server IP address)

Once BootP is initiated, the TRMM transmits a BootP request to the BootP server on its network in order to receive a BootP response (from the server). The BootP server first attempts to match the TRMM's MAC address to the MAC address defined in the bootptab file:

- If the MAC addresses match, the BootP server responds to the BootP request by transmitting the information to the TRMM.
- If the MAC addresses do not match, no action is taken by either the TRMM or the BootP server.

If the TRMM's current configuration differs from the configuration information contained in the BootP response, the TRMM updates its configuration as specified in the response.

In addition, if the response contains valid TFTP variables (as defined above) with a file type set to ASCII, the TRMM performs a TFTP to the server IP address, downloads the script file specified by the TFTP filename, and executes this script.

Starting BootP

BootP can be initiated automatically upon startup of the TRMM or initiated manually using a management command. Use the SET BOOTP POWER_UP_MODE ENABLE command to have the TRMM initiate a BootP request upon startup, or use the BOOTP command to initiate a BootP request at any time.

You can also define the BootP server IP address to which the TRMM should send its BootP request. If you do not specify a BootP server IP address, the TRMM sends out the request to the broadcast address.

If BootP is enabled upon startup of a master TRMM, and the TRMM cannot locate the server on its current network, it determines to which networks Token Ring modules in the hub are connected (because these are the only available path to a server). The TRMM then connects to each of these networks, starting with the next network from the one it is currently configured, until a BootP server is located (that is, if the TRMM is configured to Token Ring 3, it assigns itself next to Token Ring 4).

If the TRMM is a slave, it only attempts to locate a BootP server on its current network.

If a master or slave TRMM cannot locate a BootP server, the BootP result displays No Response.

Showing BootP Settings

Use the SHOW BOOTP command to display the current BootP configuration settings.

```
8250> show bootp
——-   BOOTP VARIABLES    ——-
BootP Server IP address:  127.36.58.53
BootP Power Up Mode:      enabled
BootP Result:             Okay
```

Clearing the BootP Result

Use the CLEAR BOOTP command to clear the BootP result.

```
8250> clear bootp result
```

Sample BootPtab File

A sample bootptab file is shown below. This file is created on the BootP server. Comments are entered after the pound sign (#).

```
#/ect/bootptab: database for bootp server (/ect/bootpd)
#Blank lines and lines beginning with '#' are ignored.
#
#Legend:
#
# first field – host name
#
#   hd – home directory
#   bf – bootfile
#   cs – cookie servers
#   ds – domain name servers
#   gw – gateways
#   ha – hardware address
#   ht – hardware type
#   im – impress servers
#   ip – host IP address
#   lg – log servers
#   lp – LPR servers
#   ns – IEN-116 name servers
#   rl – resource location protocol servers
#   sm – subnet mask
#   tc – template host (points to similar host entry)
#   to – time offset (seconds)
#   ts – time servers
#
#   IBM Vendor specific definitions:
#
#   T140 – TFTP server file name
#   T141 – TFTP server file type
#     0x01 = FLASH
#     0x02 = BOOT
#     0x03 = ASCII
#   T142 – TFTP server IP address

IBM 5200M:ip=151.104.12.125:ht=ieee802:ha=100f10f0c68:\
sm=0xffffff00:gw=0x97680c01 0x97680c02:T140="/dhome/davies/script3":\
T141=0x03:t142=0x97680C12
```

Using Scheduling

The Scheduling feature allows you to execute scripts at a specific time of day, or days of the week or month. A maximum of 20 schedules can be defined for each TRMM. Each schedule needed to run a script automatically must be configured to include the following information:

- Schedule identification number
- Time of day a script is to run
- Identification number of the script
- Day or group of days a script is to run

Scheduling also enables you to define three different schedule groups, Weekday, Weekend, and Holiday, which contain days or dates. These days or dates may identify a typical work week, weekend, and holiday schedule for the organizations in your company.

Once a group is defined, you can include it in a schedule's configuration. A schedule will then execute a script on the days or dates specified in a group. Schedule groups save you time when configuring schedules by enabling you to associate a group with a schedule, rather than your having to input each day or date into a new or existing schedule.

Scheduling Examples

The following scheduling command examples describe how to set up three schedules to enable and disable user ports at specific times, days, and dates.

Schedule 1 is configured to:

- Execute script 1 (which enables all user ports)
- Execute script 1 every day (except Sunday) at 6:00 am (accomplished by associating the user-defined Weekday group with schedule 1)

Schedule 2 is configured to:

- Execute script 3 (which disables all user ports)
- Execute script 3 every weekday at 6:00 pm (accomplished by associating the user-defined Weekday group with schedule 2)

Schedule 3 is configured to:

- Execute script 3 (which disables all user ports)
- Execute script 3 on all dates specified in the Holiday group at noon

1. Define schedules 1, 2, and 3 by specifying the schedule number, the time a script is to execute, and the script number that is to execute.

```
8250> set schedule 1 time 06:00 script 1
8250> set schedule 2 time 18:00 script 3
8250> set schedule 3 time 12:00 script 3
```

2. Set up a Weekday schedule group.

   Use the following commands to define a Weekday group consisting of Monday through Saturday.

```
8250> set schedule weekday include_day monday
8250> set schedule weekday include_day tuesday
8250> set schedule weekday include_day wednesday
8250> set schedule weekday include_day thursday
8250> set schedule weekday include_day friday
8250> set schedule weekday include_day saturday
```

3. Set up a Holiday schedule group. A holiday group can contain a maximum of 10 entries.

```
8250> set schedule holiday include_date 12/25
8250> set schedule holiday include_date 12/26
8250> set schedule holiday include_date 1/1
```

4. Associate schedules 1, 2, and 3 with their schedule groups.

```
8250> set schedule 1 include_day weekday
8250> set schedule 2 include_day weekday
8250> set schedule 3 include_date holiday
```

5. Enable schedules 1, 2, and 3.

```
8250> set schedule all mode enable
```

6. Use the SHOW SCHEDULE command to display all schedule configurations.

```
8250> show schedule all
Schedule                    Script     Days
Index     Mode       Time   Number     MTWTFSS    Dates
_____     ____       ____   ______-    _______    _______
1         ENABLED     6:00    1       ++++++
2         ENABLED    18:00    3       ++++++
3         ENABLED    12:00    3                  +HOLIDAY
```

Using Scripting

The Scripting feature enables you to create a command file by specifying a list of management commands to be executed. Scripts can be executed by invoking a specific command or in response to a threshold event or schedule. You must be logged in under the Super User password in order to execute scripts.

All TRMM commands can be executed from a script file with the exception of the following commands:

- BOOTP
- DOWNLOAD
- MAINTAIN
- MONITOR
- PING
- TELNET

Each TRMM allows a maximum of eight scripts. The TRMM checks the syntax of a script file when the script is executed. Misspelled entries or invalid commands cause the script execution to be aborted.

A single script file can be a maximum of 15 lines with 72 characters allowed per line. Comment fields are allowed in the command lines. Comments may start anywhere on the command line but must be preceded by a pound sign (#). All text following the pound sign until the end of the line is ignored. Comments that span more than one line are counted as part of the 15-line maximum.

Use the SET ALERT SCRIPT command to enable or disable trap generation when a script executes. If enabled, traps are generated for both of these conditions (nested abort and recursive abort). The trap contains the script number, script name, how the script was executed (RUN command or defined threshold), and the script execution status (OK, Abort, Nested Abort, Recursive Abort).

Script output from the RUN SCRIPT command is displayed at the originating terminal or workstation.

Nesting Scripts

Scripts are allowed to invoke other scripts. The TRMM supports a maximum of four levels of embedded scripting. Once an embedded script has completed execution, it returns control to the script that invoked it. If the maximum embedded call level is reached, that command line is ignored and script execution continues to the next command line.

Note that a script is not allowed to call itself (recursion is not allowed). If a script calls itself, that command line is ignored and script execution continues on to the next command line.

Downloading Scripts

You can also download script files using TFTP (Trivial File Transfer Protocol). The SET TFTP FILE_TYPE command has an ASCII option, which allows you to download a script file from a workstation or personal computer to the TRMM. A script file that is downloaded must contain the header SCRIPT (which does not count as part of the 15-line maximum). A script file to be downloaded should also contain a script name and script identification number next to the SCRIPT header.

Note that if you define a script number as a number that already exists, the TRMM downloads the new script over the existing script, thus overwriting the existing script. If the script number is not defined, the script file is copied into the next available script on the TRMM. If the maximum number of scripts on a TRMM (eight) is reached, the script file is not stored.

Scripting Examples

The following command examples show how to create and name a script. This sample script contains five SET commands, is defined as script 1, and identified as ENG3.

```
8250> set script 1 insert 1

Enter line(s) to insert. Enter a blank line to quit this mode.
```

```
set port 12.2 mode enable
set port 17.1 mode enable
set bootp power_up_mode enable
set tftp file_type ascii
set tftp file_name
/tftpboot/script1
```

```
8250> set script 1 name ENG3
```

Use the SHOW SCRIPT VERBOSE command to display the contents of the script file.

```
8250> show script 1 verbose

Script Number:1    Script Name: ENG3
1 set port 12.2 mode enable
2 set port 17.1 mode enable
3 set bootp power_up_mode enable
4 set tftp file_type ascii
5 set tftp file_name
6 /tftpboot/script1
```

Using the TRMM Advanced Port Groups

The TRMM Advanced provides the Port Group feature, which lets you enable or disable user-defined groups of ports with a single management command. Disabling individual ports can be time-consuming. By using management commands to define a group of ports, you can issue a single command to disable or enable all of the ports in that group.

For example, if a specific department is not scheduled to work on the weekend and you want to disable each of its assigned ports, you can define all associated ports as a group. You can then issue one command to disable the ports for that entire department. Before the next work day, you need to issue only one command to enable all of the ports in that group.

You can define up to eight port groups (group_1 through group_8) within a single hub. Port groups can be defined across multiple rings, but must be within the same hub. Each group can contain an unlimited number of ports. A port can belong to more than one port group. Note that *logical* ports (for example, TRMM or bridges) *cannot* be assigned to a port group.

Port Group Examples

The following examples show how to:

- Define a group
- Name a group
- Enable the ports in a group
- Display the ports in a group
- Remove port entries from a group

Use the following commands to add ports 6, 7, 9, and 11 in the module in slot 3 to group_1:

```
8250> set group group_1 port 3.6
8250> set group group_1 port 3.7
8250> set group group_1 port 3.9
8250> set group group_1 port 3.11
```

Use the following command to rename group_1 to ENG36:

```
8250> set group group_1 ENG36
```

Use the following command to enable all of the ports in group_1:

```
8250> set group group_1 mode enable

Port 03.6 set to ENABLED.
Port 03.7 set to ENABLED.
Port 03.9 set to ENABLED.
Port 03.11 set to ENABLED.
```

Use the following command to display the ports in group_1:

```
8250> show group group_1

Group Display:

Group      Ports
group_1    3.6 3.7 3.9 3.11
```

The CLEAR GROUP command enables you to clear one port, to clear all ports on a module, to clear all ports from a specific group, or to clear the ports in all groups. Use the following command to remove all port entries from group_1:

```
8250> clear group group_1 port 3.all

Port 3.6 cleared from group_1.
Port 3.7 cleared from group_1.
Port 3.9 cleared from group_1.
Port 3.11 cleared from group_1.
```

Clearing Module Groups for Removed Modules (TRMM Advanced Only)

The TRMM Advanced provides a command that enables you to clear a port group, or all groups for a module (or modules), that has been removed. A defined port group is *not* deleted when the modules associated with the ports are removed. This feature provides you with the flexibility to remove modules without disrupting port group assignments. For example, if you replace a 20-port module whose ports are defined as group_1 with another 20-port module, the ports on the new 20-port module are now defined as group_1.

This feature also allows you to replace a module with a different type of module. For example, if you replace a 20-port module whose ports are defined as group_2 with an 8-port module and then issue the CLEAR GROUP PORT NON_EXISTING command, ports 1 through 8 remain in group_2 and ports 9 through 20 are cleared from group_2.

For example, use the following command to clear a removed module's ports from group_1:

```
8250> clear group group_1 port non_existing

Port 3.6 cleared from group_1.
Port 3.7 cleared from group_1.
Port 3.9 cleared from group_1.
Port 3.11 cleared from group_1.
```

Using the TRMM Advanced Thresholds

TRMM Advanced enables you to specify threshold settings for:

- Network counters
- Port counters
- Station counters

Once you have set these thresholds, the TRMM monitors the associated counters at selected (user-defined) intervals. At the end of each interval, the value at the end of the interval is subtracted from the value at the *beginning* of the interval, and the difference is compared to the threshold value specified in the SET THRESHOLD VALUE command. When the counter exceeds the threshold value you have specified, an SNMP trap is sent notifying the management station.

Note: Because the TRMM does not collect per-port counter statistics when in RMON probe mode, this feature does not work with probe mode enabled.

The TRMM sends additional traps each time the value drops below *then exceeds* the threshold. If the value is consistently above the threshold, the TRMM does not send additional traps.

For example, if you specify a Threshold Value of 100 for an Interval of 60 seconds, the TRMM sends a trap if the specified counter value reaches 101 during the 60-second period. If the counter again exceeds 100 during the next interval, the TRMM does not send a second trap.

Each threshold you set is counted as a separate entry, identified by the index parameter, and entered in the threshold table.

Note: Thresholds can be set on a port regardless of whether the port has a device connected to it, or whether the port is enabled or disabled.

Threshold Examples

The following examples show how to set up a threshold with the following requirements:

- Define index 1 as network frames
- Define a threshold value of 3000 frames
- Define frames to be checked at 2-minute intervals
- Enable index 1
- Define the action the TRMM is to take when the threshold is exceeded
- Describe index 1
- Save all threshold information
- Show index 1 configuration (threshold information for an index entry is displayed each time a command for that index entry is issued)

```
8250> set threshold 1 network frames
8250> set threshold 1 value 3000
8250> set threshold 1 interval 2 minutes
8250> set threshold 1 mode enable
8250> set threshold 1 action script_trap
8250> set threshold 1 description
> This threshold is for network frames
8250> save threshold
8250> show threshold 1

Index:                        1
Mode:                         Script Trap
Description:                  This threshold is for network frames
Data Source:                  Network TOKEN_RING_1 : Frames
Threshold Value:              3000
Current Value:                2136
Interval:                     0:02:00
Time Since Last Triggered:    3:17
```

In this example, the Current Value entry reports the number of network frames as of the last interval. Issue the REVERT THRESHOLD command to return to any unsaved threshold settings.

```
8250> revert thresholds
```

Configuring Fiber Trunk Redundancy

This section contains the following sections:

- Fiber Trunk Redundancy Description
- Configuring Trunk Redundancy
- Configuring Ring-In and Ring-Out Fiber Trunks
- Fiber Trunk Redundancy Examples
- Displaying Trunk Redundancy
- Removing Trunk Redundancy

Fiber Trunk Redundancy Description

The fiber trunk redundancy feature:

- Allows you to configure redundant trunks using the fiber Ring-In and Ring-Out trunks on two different Token Ring Fiber Repeater Modules (Model number 3822TR) in a hub
- Provides full redundancy for the 3822TR fiber trunks

You can configure redundancy on one or both of the Ring-In and Ring-Out fiber trunks. Once you establish a redundant trunk, it becomes active only when the primary trunk fails. The TRMM supports trunk redundancy only for modules that reside in the same hub.

Note: If both the Ring-In and the Ring-Out fiber trunks on the same module are configured for redundancy, a switchover occurs only when *both* trunks fail. This feature prevents the ring from segmenting.

Configuring Trunk Redundancy

When you configure redundancy between 3822TR module fiber trunks, the following requirements apply:

1. When using 3822TR modules to connect two hubs, you can configure redundancy only for the modules in one of the hubs. Configuring redundant modules in one hub to redundant modules in the second hub may create timing inconsistencies with trunk synchronization.

2. To configure both the Ring-In and Ring-Out fiber trunks of a 3822TR module for redundancy, you must configure both trunks to be redundant to the same module.

   For example, if you configure the Ring_In.1 trunk on the 3822TR module in slot 1 to be redundant to the 3822TR module in slot 3, then you must also configure the Ring_Out.1 trunk on the 3822TR module in slot 1 to be redundant to the 3822TR module in slot 3.

The SET TRUNK command has the following syntax:

```
set trunk slot ring_in.1   mode non_redundant slot
                   out.1       redundant
```

The following example shows how to establish trunk redundancy on Ring_In.1 between the 3822TR modules in slots 1 and 3:

```
8250> set trunk 1 ring_in.1 mode redundant 3
```

In this example, the module in:

- Slot 1 is the primary trunk and is enabled.
- Slot 3 is the redundant trunk and is disabled.

If this module in slot 1 fails or if the Ring-In trunk fails, the TRMM:

- Enables the redundant trunk on the module in slot 3 (making the module in slot 3 the primary trunk)
- Disables the trunk on the module in slot 1

Ring Integrity

In addition to enabling the redundant trunk and disabling the primary trunk, the TRMM also performs the following functions to ensure ring integrity. Ring integrity prevents the ring from segmenting.

1. Because the module in slot 3 may not have a valid connection, the TRMM monitors the trunk for 10 seconds.
2. If the trunk does not establish a valid connection, the TRMM switches between the primary and redundant trunks every 10 seconds until a valid connection is established.
3. Once the TRMM establishes a valid connection, the trunk remains enabled until a failure condition occurs.

Note: If both the Ring-In and Ring-Out fiber trunks on the module in slot 1 are configured to be redundant with the module in slot 3 and a failure occurs on the Ring-In trunk only, a switchover does not occur.

4. The 3822TR module still performs a wrap on the failed Ring-In trunk to maintain the integrity of the ring.

Configuring Ring-In and Ring-Out Fiber Trunks

The TRMM protects the network from ring segmentation by preventing you from configuring the Ring-In and Ring-Out fiber trunks on the same 3822TR module to be both primary and redundant. If you attempt to configure one trunk for primary and one trunk for redundancy on the same module (an invalid configuration), an error message displays and the command is aborted.

For example, to configure Ring_In.1 of the module in slot 1 for redundancy with Ring_In.1 of the module in slot 3, enter the following command:

```
8250> set trunk 1 ring_in.1 mode redundant 3
```

To configure Ring_Out.1 of the module in slot 1 for redundancy with Ring_Out.1 of the module in slot 3, enter the following command:

```
8250> set trunk 1 ring_out.1 mode redundant 3
```

In this example, you cannot configure Ring_Out.1 of the module in slot 3 for redundancy with Ring_Out.1 of the module in slot 1 because you already issued the command to configure Ring_In.1 of the module in slot 1 for redundancy with Ring_In.1 of the module in slot 3. Configuring Ring_In.1 of the module in slot 1 for redundancy with Ring_In.1 of the module in slot 3 makes the module in slot 1 the primary module.

Warning: When you configure redundancy using the *Ring-In* fiber trunk of a primary 3822TR module, ensure that you connect the corresponding *Ring-In* fiber trunk of the redundant module to another 3822TR module.

Warning: When you configure redundancy using the *Ring-Out* fiber trunk of a primary 3822TR module, ensure that you connect the corresponding *Ring-Out* fiber trunk of the redundant module to another 3822TR module.

Fiber Trunk Redundancy Examples

Figure 5-1 illustrates two 3822TR modules configured for redundancy using the Ring-In fiber trunks.

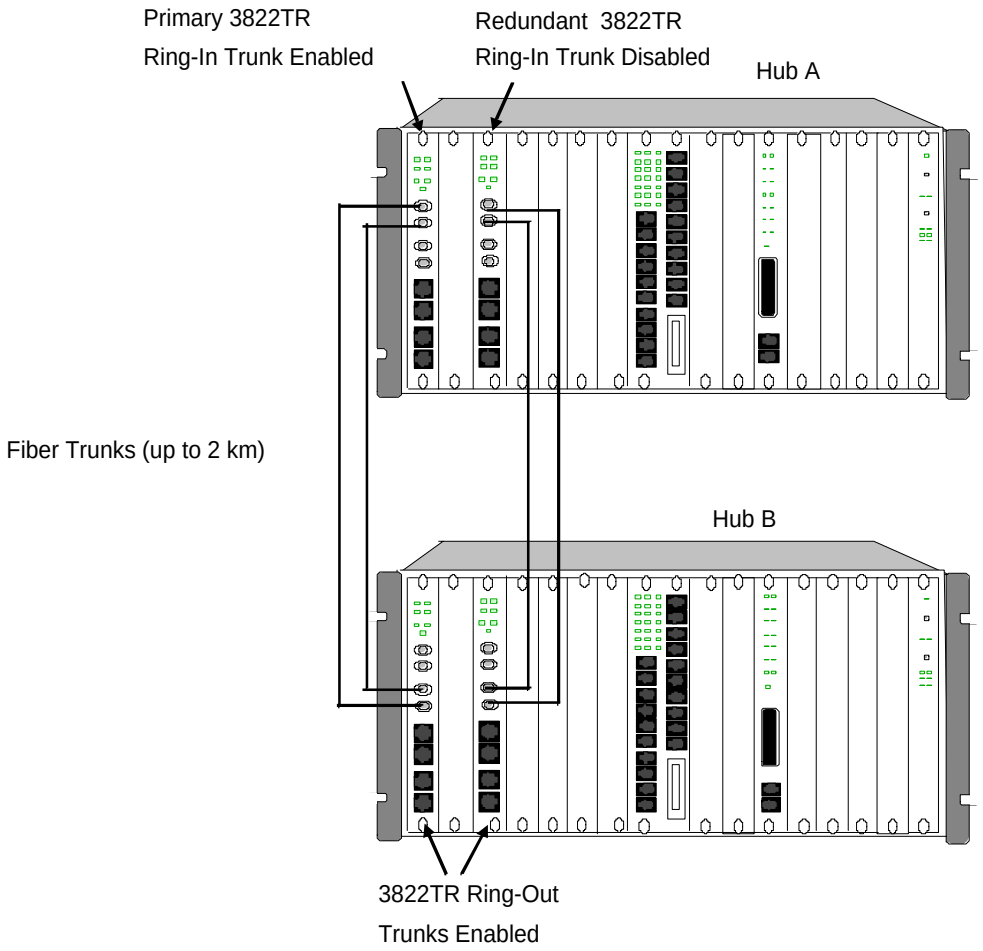


Figure 5-1. 3822TR Modules Configured for Fiber Redundancy Using Ring-In Fiber Trunks

The configuration in Figure 5-1 is described below.

In Hub A:

- The Ring-In fiber trunk of the 3822TR module in slot 3 is configured for redundancy to the Ring-In fiber trunk on the 3822TR module in slot 1.
- The 3822TR module in slot 1 is connected to the 3822TR module in slot 1 of Hub B.
- The 3822TR module in slot 3 is connected to the 3822TR module in slot 3 of Hub B.
- The 3822TR module in slot 1 is assigned to the same backplane network as the 3822TR module in slot 3.

In Hub B, the 3822TR module in slot 1 is assigned to the same backplane network as the 3822TR module in slot 3.

If the Ring-In fiber trunk of the 3822TR module in slot 1 of Hub A experiences a failure, the TRMM:

- Disables the Ring-In fiber trunk of the 3822TR module in slot 1
- Performs a switchover to the 3822TR module in slot 3 (Hub A)

The newly assigned primary 3822TR module in slot 3 of Hub A maintains ring integrity through its connection to the 3822TR module in slot 3 of Hub B.

The 3822TR module in slot 3 of Hub B, which is assigned to the same network as the 3822TR module in slot 1 (Hub B), passes traffic over the backplane to the 3822TR module in slot 1 (Hub B).

Figure 5-2 illustrates two 3822TR modules configured for redundancy using both the Ring-In and Ring-Out fiber trunks.

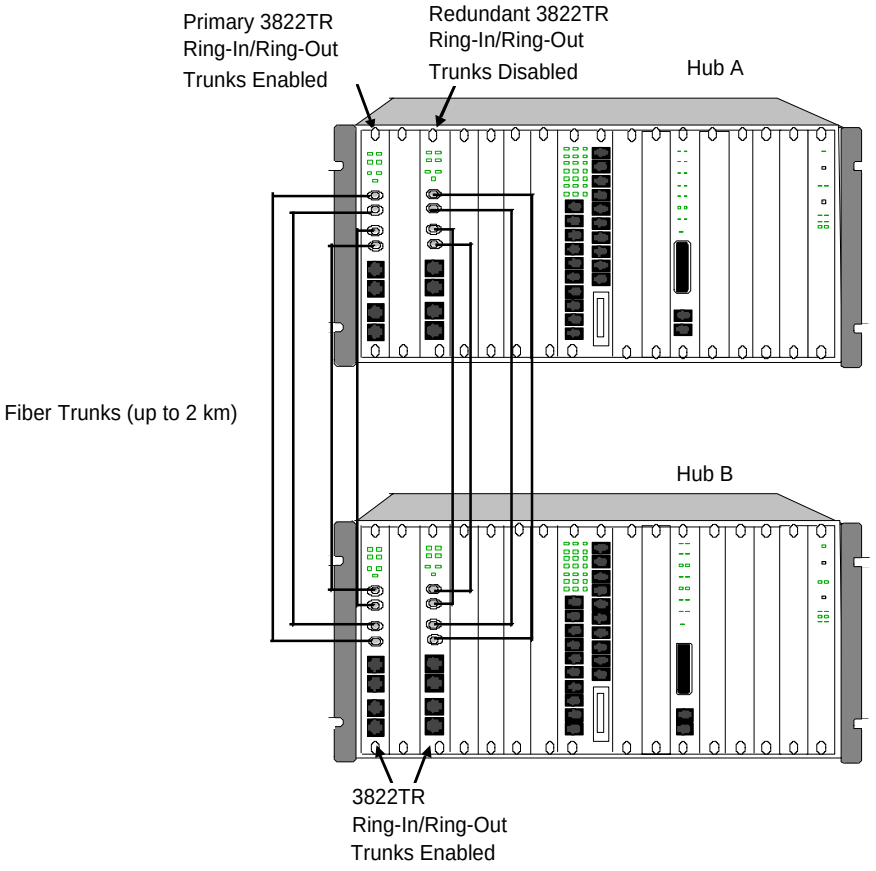


Figure 5-2. 3822TR Modules Configured for Fiber Redundancy Using Both Ring-In and Ring-Out Fiber Trunks

The configuration in Figure 5-2 is described below.

In Hub A:

- The Ring-In and Ring-Out fiber trunks of the 3822TR module in slot 3 are configured for redundancy to the Ring-In and Ring-Out fiber trunks on the 3822TR module in slot 1.

- The 3822TR module in slot 1 is connected to the 3822TR module in slot 1 of Hub B.
- The 3822TR module in slot 3 is connected to the 3822TR module in slot 3 of Hub B.
- The 3822TR module in slot 1 is assigned to the same backplane network as the 3822TR module in slot 3.
- The 3822TR module in slot 3 is connected to the 3822TR module in slot 3 of Hub B.

In Hub B, the 3822TR module in slot 1 is assigned to the same backplane network as the 3822TR module in slot 3.

If both the Ring-In and Ring-Out fiber trunks of the 3822TR module in slot 1 of Hub A experience a failure, the TRMM:

- Disables the Ring-In and Ring-Out fiber trunks of the 3822TR module in slot 1
- Performs a switchover to the 3822TR module in slot 3 (Hub A)

The newly assigned primary 3822TR module in slot 3 of Hub A maintains ring integrity through its connection to the 3822TR module in slot 3 of Hub B.

The 3822TR module in slot 3 of Hub B, which is assigned to the same network as the 3822TR module in slot 1 (Hub B), passes traffic over the backplane to the 3822TR module in slot 1 (Hub B).

Displaying Trunk Redundancy

To display trunk redundancy information, enter the SHOW TRUNK command:

```
8250> show trunk all
Trunk Display for Module 3822TR:
Slot Trunk      Mode     Status      Network        General Information
---- ---------- -------- ----------- -------------  -----------------
 1   RING_IN.1  PRIMARY  OKAY         TOKEN_RING_1   Active; Buddy:
 1   RING_OUT.1 DISABLED NO CABLE    TOKEN_RING_1
 1   RING_IN.2  DISABLED NO SQUELCH  TOKEN_RING_1
 1   RING_OUT.  DISABLED NO SQUELCH  TOKEN_RING_1
 1   BP_IN      ENABLED  OKAY         TOKEN_RING_1   TR_PATH_2
 1   BPL_OUT    ENABLED  OKAY         TOKEN_RING_1   TR_PATH_4

— More —
Trunk Display for Module 3822TR:
Slot Trunk      Mode     Status     Network        General Information
---- ---------- -------- ---------- -------------  -----------------
 3   RING_IN.1  STANDBY  OKAY       TOKEN_RING_2   Standby; Buddy: 01
 3   RING_OUT.1 DISABLED NO CABLE   TOKEN_RING_2
 3   RING_IN.2  DISABLED NO SQUELCH TOKEN_RING_2
 3   RING_OUT.2 DISABLED NO SQUELCH TOKEN_RING_2
 3   BP_IN      ENABLED  OKAY       TOKEN_RING_2   TR_PATH_4
 3   BP_OUT     ENABLED  OKAY       TOKEN_RING_2   TR_PATH_12
```

Removing Trunk Redundancy

To remove trunk redundancy between the modules in slots 1 and 3, enter the following command:

```
8250> set trunk 1 ring_in.1 mode non_redundant
```

You can also remove redundancy by enabling or disabling the mode of either trunk. Enabling or disabling trunks automatically removes redundancy configurations.

When you configure a module for redundancy and then remove the module from the hub, or if the module fails:

- The trunk on the remaining redundant module remains enabled (or becomes enabled if previously disabled).
- The redundant configuration is removed.

Using the SHOW Commands

You can use SHOW commands to display configuration information for the following:

- Concentrator
- Module
- Network
- Counter
- Device (TRMM)
- Port
- Log

All MAC addresses are displayed in Token Ring format. This includes Ethernet MAC addresses that are bridged to a Token Ring network. Ethernet modules with associated MAC addresses (for example, bridges and terminal servers) have their address displayed in Token Ring format. When sent from the TRMM, SNMP always returns addresses in *canonical* format.

Canonical order is defined by IEEE 802.1a and specifies MAC addresses with the least significant bit first. The IEEE 802.5 Token Ring protocol, in contrast to other 802.x protocols, specifies the most significant bit first. For example, the MAC address 10-00-F1-0F-0C-72 in Token Ring format would be equivalent to 08-00-8F-F0-30-4E in canonical format.

Showing Hub Information

Use the SHOW CONCENTRATOR command to report the status of the primary and backup power supplies and temperature status for the hub:

```
8250> show concentrator
Concentrator Information:
Concentrator Type: 8250-017
Primary power supply status: NORMAL
Backup power supply status:  NORMAL
Temperature sensor status:   NORMAL
```

Showing Device Information

Use the SHOW DEVICE command to display the current TRMM information, including the information you can modify:

```
8250> show device
T01MS Token Ring Management Module (Advanced-MGT) v4.00-A pSOS+ SNMP

Name:  8250
Location:  Unknown
For assistance contact:
  System Administrator

Boot EPROM Version:  v3.03-A    Size:  256 KBytes
Flash EPROM Version: v4.00-A    Size: 1024 KBytes  DRAM Size: 2048 KBytes
Serial Number:                     Service Date:  95/02/27    Restarts: 124

Network     IP Address       Subnet Mask   Primary Gateway  Secondary Gateway
--------    --------------   -----------   ---------------  -----------------
tr_1     *  151.104.25.141   FF.FF.FF.00   0.0.0.0        * 0.0.0.0
tr_2        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_3        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_4        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_5        151.104.25.141   FF.FF.FF.00   0.0.0.0          0.0.0.0
tr_6        151.104.25.141   FF.FF.FF.00   0.0.0.0          0.0.0.0
tr_7        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
isolated    151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0

MAC Address: 10-00-F1-0F-23-FC  Beacon Trunk Retry:  0 time(s)
Dip Configuration:  DISABLED    Diagnostics:         ENABLED
Trap Receive:       DISABLED    Beacon Recovery:     ENABLED
Monitor Contention: ENABLED     Beacon Timeout:      10 second(s)
```

Showing Module Information

Use the SHOW MODULE ALL command to view information about all of the modules currently installed in the hub:

```
8250> show module all

Slot Module      Version  Network        General Information
 01  C00NS-RCTL  003      N/A
 03  T20MS-RJ45S 001      TOKEN_RING_1   Port(s) are down
 05  T20MS-RJ45S 001      ISOLATED
*15  T01MS-MGTA  v4.00    TOKEN_RING_1   Master Management Module
```

In this example, the slots are occupied as follows:

- Slot 1 contains a Controller Module.
- Slot 3 contains a Token Ring 20-Port Module on network 1.
- Slot 5 contains a Token Ring 20-Port Module that is isolated.
- Slot 15 contains a master TRMM Advanced module operating on Token Ring network 1. The asterisk (*) at slot number 15 of the example indicates the TRMM with which you are currently communicating.

For additional information about a module,use the SHOW MODULE VERBOSE command. The example below displays more detailed information about the TRMM in slot 15.

```
8250> show module 15 verbose

Slot Module      Version  Network       General Information
15   T01MS-MGTA  v4.00    TOKEN_RING_1  Master Management Module

T01MS-MGT: 8250 Token Ring Management Module

Mastership Priority:                    10
Master Network:                         NO_CHANGE
Station Address:                        10-00-F1-0F-0C-7C
Ring Speed:                             16 MBPS
Network Status:                         OKAY
Locally Administered Address:           00-00-00-00-00-00
MAC Address Type:                       BURNED-IN
Active MAC Address:                     10-00-F1-0F-0C-7A
```

Showing Port Information

The TRMM enables you to display the status of all module ports. Use the SHOW PORT command to display the mode and status of all ports, or to display the mode and status of a specific port.

The following example displays information for all ports on the Token Ring MAU Module in slot 3.

```
8250> show port 3.all

Port Display for Module T08MS-RJ45S:

Port   Mode     Status       Network       General Information
03.01  ENABLED  OKAY         TOKEN_RING_3
03.02  ENABLED  LINK FAILURE TOKEN_RING_3  Port is down
03.03  ENABLED  OKAY         TOKEN_RING_3
03.04  ENABLED  OKAY         TOKEN_RING_3
03.05  ENABLED  OKAY         TOKEN_RING_3
03.06  ENABLED  OKAY         TOKEN_RING_3
03.07  ENABLED  OKAY         TOKEN_RING_3
03.08  ENABLED  OKAY         TOKEN_RING_3
```

You can also display detailed information about a specific port using the SHOW PORT VERBOSE command.

```
8250> show port 15.1 verbose

Port Display for Module T01MS-MGT:

Port  Mode     Status       Network        General Information
15.01 LOGICAL  OKAY         TOKEN_RING_1

Port Connector:           BACKPLANE
IP Address:               151.104.12.105
```

Showing Network Information

The TRMM provides an important mapping feature that enables you to maintain a detailed topological map of the 8250 Multiprotocol Intelligent Hub and its Token Ring modules. When a TRMM is assigned to a Token Ring network, it builds an information base for mapping the ring. This base includes information about ring topologies, modules, slot numbers, and MAC addresses for each station on the ring. You can use the SHOW NETWORK_MAP TOKEN_RING command as shown below to display various aspects of network operation.

Use the SHOW NETWORK_MAP TOKEN_RING LOGICAL command to display information about ring topology and identify which port is the active monitor:

```
8250> show network_map token_ring logical

Token Ring Logical Map

MAC Address            Slot           Port
10-00-f1-0f-0c-63       7               1
10-00-90-28-4d-52       3               20   <- Active Monitor
10-00-90-28-30-e0       3               10
08-00-20-10-61-4d       3               1
```

Use the SHOW NETWORK_PATHS command to display a list of the logical network assignments and their corresponding physical backplane path connections:

```
8250> show network_paths token_ring

Physical Path            Logical Network
_______-                 ________
TR_PATH_1                TOKEN_RING_1
TR_PATH_2                available
TR_PATH_3                available
TR_PATH_4                available
TR_PATH_5                available
TR_PATH_6                available
TR_PATH_7                TOKEN_RING_3
TR_PATH_8                available
TR_PATH_9                available
TR_PATH_10               available
TR_PATH_11               available
TR_PATH_12               TOKEN_RING_1
TR_PATH_13               available
TR_PATH_14               available
TR_PATH_15               available
```

Refer to the *8250 Management Commands Guide* for a complete description of the SHOW NETWORK command and its available options.

Showing Counter Statistics

Once the TRMM is assigned to a network, it continuously records and updates error statistics on all Token Ring stations, ports, and the network to which it is assigned. The SHOW COUNTER command can be issued for the device (TRMM), or for a specific station, port, or network.

Note: TRMM automatically disables this feature when RMON statistics are enabled.

Note: Counter displays include all frames that have valid lengths (including error frames). Because counters include error frames, stations that do not exist may appear in SHOW COUNTER command displays. This situation most commonly occurs when a trunk goes up or down. If extraneous stations display, issue the CLEAR COUNTER ALL command.

Octet counters may overflow under certain conditions. If, for example, your network is running at 16 Mbps and 50% utilization, octet counters overflow after about 70 minutes. When you issue any SHOW COUNTER command, a warning message displays alerting you that some counters have overflowed. Counters that overflow reset back to 0 and continue counting. If this situation occurs, issue the CLEAR COUNTER ALL command to reset all counters back to 0.

The Time Since Cleared field within individual station or port traffic counter displays indicates either the time since the station or port counter was cleared or the time since the station or port was discovered by the TRMM (whichever occurred last). Consequently, the time displayed in this field may be different across station or port traffic counter displays.

Use the following command to report error and traffic statistics for the TRMM:

```
8250> show counter device
Slot 14, Port 1 MAC Address 10-00-f1-0f-0c-6a
ERROR COUNTERS:
        Line Errors:                          0
        Burst Errors:                         3
        Address/Frame Errors:                 0
        Lost Frame Errors:                    0
        Receive Congestion Errors:            1
        Frame Copy Errors:                    0
        Token Errors:                         0
TRAFFIC COUNTERS:
        Inbound Octets:                       1218
        Inbound Unicast Packets:              0
        Inbound Non-Unicast Packets:          348
        Inbound Discarded Packets:            0
        Inbound Error Packets:                0
        Outbound Octets:                      16708
        Outbound Unicast Packets:             0
        Outbound Non-Unicast Packets:         17
        Outbound Discarded Packets:           0
        Outbound Error Packets:               0
```

In addition to recording error counters for devices, ports, and stations, the TRMM Advanced module records traffic statistics for network, ports, and stations.

The TRMM Advanced module also provides commands that enable you to display the following statistics for the most active stations:

- A summary of errors received by each station on the network (SHOW COUNTER TOP_ERRORS)
- A summary of traffic statistics received by each station on the network (SHOW COUNTER TOP_RECEIVERS)
- A summary of traffic statistics transmitted by each station on the network (SHOW COUNTER TOP_SENDERS)

These options can be displayed by frames, MAC address, or octets (octets not available for Top Errors).

Use the following command to display top receiver counters by MAC address for all stations.

```
8250> show counter top_receivers by_mac_address all
Station Traffic Statistics - sorted by Top MAC Address - at 7:28 Fri 19 Jan 96

MAC Address        Slot.Port         Since Cleared  Frames     Octets  Pct
00-00-00-00-00-60  REMOTE            0:28:07             1      20492   2.54%
00-00-00-01-20-14  REMOTE            0:31:59             1      27556   3.42%
00-18-00-00-89-D0  REMOTE            0:17:57             1      27067   3.36%
08-01-20-0F-AA-DD  REMOTE            0:31:58            18       2365   0.29%
10-00-F1-0F-0C-63  REMOTE            0:31:59            18       1476   0.18%
10-A0-AB-A3-18-A1  REMOTE            0:20:20             1      24446   3.03%
62-4A-4C-1C-00-00  REMOTE            0:17:14             1      13468   1.67%
C0-00-00-00-00-08  Ring Err Monitor  0:31:59           399      20616   2.56%
C0-00-00-00-00-10  Network Manager   0:31:59            40       1600   0.20%
C0-00-FF-FF-FF-FF  Broadcast         0:45:19          3509     127088  15.77%
FF-FF-FF-FF-FF-FF  Broadcast         0:31:58            56       4032   0.50%
```

Use the following command to display traffic statistics for the network to which the TRMM is assigned.

```
8250> show counter network traffic

Network Traffic Counters for ISOLATED at 11:24 Fri 19 Jan 96

Time since last clear counters: 1:11:09

Network Performance Statistics

Bandwidth   16.00 mbps       Total Number of Stations:     1

                    Current

Average frame size      36
Frames per second      0.1
Octets per second      5.2
Utilization (mbps)    0.00
Utilization ( % )     0.00

Token rotation (usec)    3
```

Use the SHOW COUNTER STATION ALL TRAFFIC command to display traffic statistics for all stations on the network. This display reports the percentage of frames and octets generated by each station on the network.

```
8250> show counter station all traffic

Station Statistics - sorted by MAC Address - at 1:28 Fri 19 Jan 96

MAC Address        Slot.Port   Since Cleared  Frames  Octets
10-00-F1-0F-0C-7A  12.01       1:14:23           641   23396 100.00%
```

Using the MONITOR Command

The MONITOR command reports the same information as the SHOW COUNTER command except that the system reports only on the events occurring for the time you specify. The information displayed by the MONITOR command is not cumulative; rather it is *current*. Use the MONITOR command periodically to report current error statistics for the TRMM Basic module, and error and traffic statistics for the TRMM Advanced module (the frequency of reporting is determined by the time, expressed in minutes, that you request).

Note: This feature automatically disables when RMON is enabled.

Use the following command to monitor traffic for port 4 on the module in slot 4 every 5 seconds:

```
8250> monitor 0:05 port 4.4 traffic

Port Traffic Statistics - at 08:15 Fri 19 Jan 96
MAC Address     08-00-20-04-FC-8D          Slot.Port    04.04
Transmitted:       Current     Minimum     Maximum    Cumulative

Average frames       36          36          36          24
Frames (total)        1           1           1           2
 Non-MAC Frames       0           -           -           -
 Multicast            0           -           -           -
 Broadcast            1           -           -           -
 Source Routed        0           -           -           -
Frames per second     0.2         0.2         0.2         0.1
Octets (total)       36          36          36          2
 Non-MAC Octets       0           -           -           -
Octets per second     7.2         7.2         7.2         4.8
Traffic Util (mbytes) 0.00        0.00        0.00        0.00
Traffic Util ( % )    0.03        0.03        0.03        0.02
Bandwidth Util ( % )  0.00        0.00        0.00        0.00
Received:
        Octets              0
        Frames              0
Display will refresh every 5 seconds.

Press CTRL-C to exit. ^C
```

Using the SET COUNTER PORT_STATISTICS Command

The SET COUNTER PORT_STATISTICS command improves network statistics reporting by allowing you to control whether or not the TRMM collects port statistics. By default, the TRMM does not collect port statistics.

To enable the TRMM to collect port statistics, use the following command:

```
8250> set counter port_statistics enable
```

- If you disable the Counter Port Statistics feature, the TRMM does not collect port statistics (the default).
- If you enable the Counter Port Statistics feature, the TRMM collects port statistics.

Note: Collecting port statistics affects network statistics reporting.

To save the SET COUNTER PORT_STATISTICS setting permanently, enter the SAVE ALL or SAVE MODULE_PORT command.

The SHOW COUNTER PORT_STATISTICS command allows you to display the current setting for the SET COUNTER PORT_STATISTICS command:

```
8250> show counter port_statistics
```

There is no SNMP support for the Counter Port Statistics feature.

Showing Trap and Event Logs

Trap and event logs store information on system events:

- **Event log** — Tracks fatal errors that occur on the TRMM
- **Trap log** — Tracks SNMP events or alerts

To display a log of stored fatal events, use the SHOW LOG EVENT_LOG command:

```
8250> show log event_log
Display of Last Error - Flash Version: vx.xx
Crash Date/Time: 05:58 Sat 2 Mar 96
Date/Time:       06:17 Sun 3 Mar 96
   -0-      -1-      -2-      -3-      -4-      -5-      -6-         -7-
A=12345678 2000044C 20000001 00000000 00000000 00000000 200D124C  200D1208
D=11111111 0000023D 00000000 00000000 00000000 00000000 00000000  00000000
  Vector = 20020494   personal computer = 20000000   SR = 3009
Stack Dump:
200D1208  00 2C 20 02 5D B6 00 00 - 00 00 00 00 00 00 00 00 .......
200D1218  00 02 20 00 00 03 00 00 - 00 00 DE AD DE AD 00 00 .......
200D1228  00 00 00 00 00 00 00 00 - 00 04 00 00 00 00 00 00 .......
200D1238  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1248  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1258  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1268  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1278  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
```

To display a list of non-fatal system events, use the SHOW LOG TRAP_LOG command:

```
8250> show log trap_log

-------------------TRAP 1 ----------------------------


Message received from this device on 15:43 Mon 22 Jul 96:

Enterprise:               IBM
Enterprise Specific trap:  Security Environment Change

Message Information:
      Security Trap Reason:  INTRUSION_ATTEMPT
       Slot Number :  3
       Port Number :  1
       Port Mode :  ENABLED
      Intruder MAC Address :  08 00 8f 30 09 0a
```

Chapter 6. Using RMON to Monitor the Network

This chapter describes 8250 TRMM support for the RMON MIB (Remote Network-Monitoring Management Information Base) and how to use RMON commands and statistics to monitor and analyze a network. This chapter contains the following sections:

- RMON MIB Overview
- Support for the RMON MIB
- Enabling and Disabling Monitoring Tasks
- Using the Host Group
- Using the Host TopN Group
- Using the Matrix Group
- Using the Statistics Group
- Using the Source Routing Group
- Using the Token Ring Ring-Station Group
- Using the Alarm and Event Groups
- Interpreting Token Ring Statistics

It is helpful to gain a basic understanding of SNMP (Simple Network Management Protocol) before you try to use the RMON MIB. The following book provides an excellent introduction to SNMP as well as a detailed discussion of the RMON MIB:

SNMP, SNMPv2, and CMIP: The Practical Guide to Network-Management Standards by William Stallings. 1993. Addison-Wesley Publishing Company.

RMON MIB Overview

The RMON MIB is a component of SNMP (Simple Network Management Protocol) that allows an SNMP agent to perform certain network monitoring and analysis functions. The RMON architecture distributes network monitoring and analysis functions between two entities:

- **RMON probe** — Monitors network activity by examining all packets sent on the network. It stores statistics and performs some types of analysis. In the 8250 TRMM, the RMON probe is part of the SNMP agent that runs on the management module.
- **RMON manager** (for example, IBM LAN ReMON application) — Collects and displays data from RMON probes and controls aspects of RMON probe operation. The RMON manager can collect data from many probes on different networks, allowing a network manager to monitor an enterprise-wide internetwork from a central location.

Support for the RMON MIB

This section defines 8250 Token Ring Module support for the RMON MIB. It contains the following sections:

- Support for RMON MIB Groups
- Accessing the RMON MIB

Support for RMON MIB Groups

The 8250 Token Ring Module RMON probe supports key groups from the RMON MIB. The groups are defined in the following IETF (Internet Engineering Task Force) RFC (Request for Comments) documents:

- *RFC 1271 - Remote Network Monitoring Management Information Base*
- *RFC 1513 - Token Ring Extensions to the Remote Network Monitoring MIB*

The RMON probe supports the following groups:

- **Host** — Information collected for particular MAC addresses (or hosts). For each packet that travels the network, the RMON probe extracts the source and destination addresses, adds the MAC addresses to the host table, and updates host-specific counters.
- **Statistics** — Current network use and error statistics. The statistics group is divided into two sections:
  - **MAC-Layer Statistics** — Information collected by observing MAC layer events.
  - **Promiscuous Statistics** — Information collected using promiscuous packet capture. In promiscuous packet capture, the RMON probe captures and analyzes all packets, not just the packets addressed to the RMON probe.

- **Host Top N** — Generates lists of hosts ordered by the host value for a selected statistic.
- **Matrix** — Records statistics for each conversation between two MAC addresses.
- **Token Ring Ring-Station** — Error statistics and status for each ring station (station on the ring), as well as ring status.
- **Token Ring Ring-Station Order** — Token-passing order for ring stations.
- **Token Ring Ring-Station Config** — Allows the RMON manager to download configuration information from ring stations, as well as reconfigure ring stations.
- **Token Ring Source Routing** — Statistics extracted from source routing information in Token Ring packets.
- **Event** — Defines a set of actions that the RMON probe can take when certain conditions occur. The RMON probe generates an event (takes an action) according to conditions defined in the alarm group.
- **Alarm** — Generates events by monitoring statistics and comparing statistical values against user-defined thresholds.

Accessing the RMON MIB

The 8250 Token Ring Module supports the following methods for accessing the RMON MIB:

- **SNMP** — RMON managers, such as IBM LAN ReMON, use SNMP commands to access the RMON MIB.
- **8250 terminal command interface** — The 8250 terminal command interface provides access to all RMON MIB groups.

Enabling and Disabling Monitoring Tasks

This section describes how to enable and disable RMON monitoring tasks. It contains the following sections:

- Enabling the TRMM RMON Probe Function
- Managing RMON Probe Resources
- Control and Data Tables

Enabling the TRMM RMON Probe Function

The command to enable TRMM RMON probe mode has the following syntax:

Note: You must have the TRMM Advanced version to use the TRMM as an RMON probe.

```
set module slot probe_mode enable
```

Note: You must log in to a slave TRMM to configure its RMON settings. You cannot configure the slave from the master TRMM.

Table 6-1 shows which TRMM statistics information is available when you enable or disable RMON probe mode.

Table 6-1. Effect on Counters When Enabling and Disabling RMON Probe Mode

TRMM Version v4.0 Counters	Is Counter Available When RMON Probe Mode Is...?	
	Enabled	**Disabled**
Mac_layer Stats	Yes	No
Promiscuous Stats	Yes	No
Host	Yes	No
Host TopN	Yes	No
Matrix	Yes	No
Event	Yes	Yes
Alarm	Yes	Yes
Ring Station	Yes	No
Ring Station Order	Yes	No
Ring Station Config	Yes	No
Source Routing	Yes	No
Show Counter/Monitor Device	Yes	Yes
Show Counter/Monitor xxx Error	Yes	Yes
Show Counter/Monitor xxx Traffic	No	Yes
Show Counter/Monitor top_errors ...	No	Yes
Show Counter/Monitor top_senders ...	No	Yes
Show Counter/Monitor top_receivers ...	No	Yes

Note: Because most TRMM-specific traffic collection is disabled when you use probe mode, thresholds that trigger based on these counters no longer work.

Managing RMON Probe Resources

You can manage RMON probe resources by selectively enabling and disabling RMON monitoring tasks according to your current needs. Depending on the size and activity level of the ring, you may find that to use certain groups effectively, you must disable all tasks in other groups. Experiment to tune RMON performance for your network.

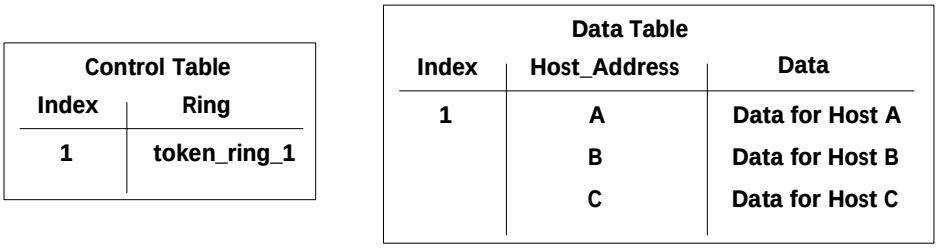
The following section describes the control and data table mechanism that controls RMON monitoring tasks.

Control and Data Tables

The RMON MIB uses control and data tables to control RMON activity and store data. Each RMON group has its own control table and data table.

Each control table entry:

- Defines a monitoring task. For example, if you are monitoring several thresholds in the alarm group, the alarm group control table contains several entries, one for each threshold. An index number identifies each control table entry.
- Has a corresponding set of data table entries. For example, a Host group control table entry defines the ring to be monitored. For each Host group control table entry, the Host group data table contains an entry for each host on the ring, as shown in Figure 6-1.



Control Table

Index	Ring
1	token_ring_1

Data Table

Index	Host_Address	Data
1	A	Data for Host A
	B	Data for Host B
	C	Data for Host C

Figure 6-1. Host Group Control and Data Tables (Simplified)

You enable a task by creating a control table entry defining that task. You disable a task by clearing (removing) the control table entry for that task.

If you are using the 8250 terminal command interface (instead of SNMP):

- Use the SET RMON command to create a control table entry.
- Use the CLEAR RMON command to clear a control table entry.

Note: The CLEAR RMON command also clears all corresponding data table entries.

Note: RMON control and data tables are stored in volatile memory. 8250 reverts to default RMON settings on re-initialization or when switched to a different backplane network.

Using the Host Group

This section describes how to use the Host group. It contains the following sections:

- Controlling the Host Group
- Viewing Host Group Data

Controlling the Host Group

This section describes how to configure the Host group.

Note: You cannot delete individual entries from the Host group data table. If the table becomes full, the RMON probe stops adding hosts to the data table.

Enabling Host Group Monitoring

At startup, the RMON agent adds an entry to the Host group control table so that host monitoring begins immediately. This control table entry is owned by the *monitor*. If this control table entry is deleted, you can enable monitoring by adding a new control table entry using the following command:

SET RMON HOST INTERFACE

For example:

```
8250> set rmon host interface
Entry 1 created.
```

Viewing the Host Group Control Table

To view a list of Host group control table entries, use the following command:

SHOW RMON HOST CONTROL ALL

For example:

```
8250> show rmon host control all
RMON Host Control Information:
Index Data Source     Table Size  Last Delete Time    Owner
----- --------------- ----------- ------------------- --------------
  1     Interface 1          89   No Deletions        monitor
```

Disabling Host Group Monitoring

To disable Host group monitoring, use the following command:

CLEAR RMON HOST

For example:

```
8250> clear rmon host all
Entry cleared.
```

Viewing Host Group Data

This section describes how to view Host group data. It contains the following sections:

- Viewing Data for All Hosts
- Viewing Data for a Single Host

Viewing Data for All Hosts

To view a list of data collected for all hosts, use the following command:

SHOW RMON HOST DATA *index* ALL *order*

Where:

- *index* specifies an entry from the Host group control table. For the 8250 TRMM, the index parameter is always 1.
- *order* specifies the order entries are sorted in. Possible values are:
  - by_creation_order
  - by_host_address

For example:

```
8250> show rmon host data 1 all by_creation_order

RMON Host display for Interface 1 :

Creation Order                  : 1
Host Address                    : 00-00-30-00-ef-b3
Input Packets                   : 0
Output Packets                  : 39229
Input Octets                    : 0
Output Octets                   : 4262499
Output Errors                   : 1
Output Packets (Broadcast)      : 6732
Output Packets (Multicast)      : 3


Creation Order                  : 2
Host Address                    : 00-00-30-80-ef-b3
Input Packets                   : 30923
Output Packets                  : 0
Input Octets                    : 1944116
Output Octets                   : 0
Output Errors                   : 1
Output Packets (Broadcast)      : 0
Output Packets (Multicast)      : 0

End of Host Table
```

Viewing Data for a Single Host

To view the information for a single host, use the following command:

SHOW RMON HOST DATA *index* HOST_ADDRESS *mac_address*

Where:

- *index* specifies an entry from the Host group control table. For the 8250 Token Ring Module, the default index is 1.
- *mac_address* is the MAC address of the host.

For example:

```
8250> show rmon host data 1 host_address 00-00-30-00-ef-b3

RMON Host display for Interface 1 :

Creation Order                  : 3
Host Address                    : 00-00-30-00-ef-b3
Input Packets                   : 0
Output Packets                  : 1465
Input Octets                    : 0
Output Octets                   : 210496
Output Errors                   : 0
Output Packets (Broadcast)      : 570
Output Packets (Multicast)      :  0
```

Using the Host Top N Group

This section describes how to use the Host Top N group. It contains the following sections:

- Controlling the Host Top N Group
- Viewing Host Top N Group Data

Controlling the Host Top N Group

This section describes how to configure the Host Top N group.

Host Top N Group Monitoring Process

Host Top N group monitoring works as follows:

1. You create a control table entry specifying the duration of the test interval and the statistic to monitor during that interval.
2. The RMON probe monitors the statistic for the specified interval. During this time the data is not available for viewing.
3. When the interval is complete, the RMON probe ranks the top 10 hosts based on the monitored statistic. You use the SHOW RMON TOPN_HOSTS command to view the data, as described below.

   The RMON probe collects no more data for this control table entry.

Enabling Host Top N Group Monitoring

At startup, the Host Top N group control table contains no entries. You enable monitoring by adding a control table entry using the following command:

SET RMON TOPN_HOSTS 1 *statistic interval*

Where:

- *statistic* is the statistic used to order the hosts. *statistic* can be one of the following:

  in_packets
  out_packets
  in_octets
  out_octets
  out_bcasts
  out_errors
  out_mcasts

- *interval* is the duration of time for which data is collected, in the format *mm:ss*.

For example, the following command specifies that the RMON probe monitor in_packets for 30 minutes:

```
8250> set rmon topn_hosts 1 in_packets 30:00
Entry 1 created.
```

Viewing the Host Top N Group Control Table

To view a list of Host Top N group control table entries, use the following command:

SHOW RMON TOPN_HOSTS CONTROL ALL

For example:

```
8250> show rmon topn_hosts control all
RMON Host Top N Control Information:
Index Data Source     Table Size  Last Delete Time    Owner
----- -------------- ----------- ------------------- -------------
   1      Interface 1         89   No Deletions        monitor
```

Disabling Host Top N Group Monitoring

To disable Host Top N group monitoring, use the following command:

CLEAR RMON TOPN_HOSTS *index*

Where:

- *index* is the control table index of the entry to be cleared. Specifying *all* clears all entries.

For example, the following command clears control table entry 1:

```
8250> clear rmon topn_hosts 1
Entry 1 cleared.
```

Viewing Host Top N Group Data

To view Host Top N group data for a specific control table entry, use the following command:

SHOW RMON TOPN_HOSTS DATA *control_table_index rank_index*

Where:

- *control_table_index* specifies an entry from the Host Top N group control table.
- *rank_index* specifies the rank of the host you want to view data for. Specifying *all* displays data for all 10 hosts.

Note: You cannot view data until the test interval is complete.

For example, the following command displays data for control table entry 3 for all 10 hosts:

```
8250> show rmon topN_hosts data 3 all
RMON Host Top N Display for Interface 1 :
Index Address           Input Packets
----- ----------------- -------------------------
1  c0-00-ff-ff-ff-ff                     1258
2  c0-00-00-00-00-02                      755
3  c0-00-00-00-00-10                      315
4  11-22-33-44-55-66                      314
5  c0-00-ff-e7-32-8b                       79
6  c0-00-00-12-14-02                       60
7  34-00-29-ef-c0-10                       42
8  9a-22-33-44-55-66                       22
9  9a-22-33-00-00-02                        0
10 34-00-29-00-00-10                        0
```

Using the Matrix Group

This section describes how to use the Matrix group. It contains the following sections:

- Controlling the Matrix Group
- Viewing Matrix Group Data

Controlling the Matrix Group

This section describes how to configure the Matrix group.

Enabling Matrix Group Monitoring

At startup, the RMON agent adds an entry to the Matrix group control table so that Matrix monitoring begins immediately. This control table entry is owned by the *monitor*. If this control table entry is deleted, you can enable monitoring by adding a new control table entry using the following command:

SET RMON MATRIX INTERFACE 1

For example:

```
8250> set rmon matrix interface 1
Entry 1 created.
```

Viewing the Matrix Group Control Table

To view the Matrix group control table, use the following command:

SHOW RMON MATRIX CONTROL ALL

For example:

```
8250> show rmon matrix control all
RMON Matrix Control Information:
Index Data Source     Table Size  Last Delete Time    Owner
----- -------------- ----------- ------------------- ---------------
   1      Interface 1         89   No Deletions        monitor
```

Disabling Matrix Group Monitoring

To disable Matrix group monitoring, use the following command:

CLEAR RMON MATRIX 1

For example:

```
8250> clear rmon matrix 1
Entry 1 cleared.
```

Viewing Matrix Group Data

To view Matrix group data, use the following command:

SHOW RMON MATRIX DATA 1 *sort_type*

Where:

- *sort_type* specifies one of the following display options:
  - **by_source_address** — Displays matrix table entries in order of source address. This is the default if you press Enter without specifying a sort_type.
  - **by_destination_address** — Displays matrix table entries in order of destination address.
  - **involving** *mac_address* — Displays only the matrix table entries containing the specified MAC address as either the source or destination address.

For example:

```
8250> show rmon matrix data 1 by_destination_address
RMON Matrix display for Interface 1 :
Source Address                  : 11-22-33-44-55-66
Destination Address             : 11-22-33-44-55-66
Index                           : 1
Packets                         : 2
Octets                          : 36
Errors                          : 0
-- More --
```

Press Enter to display the next matrix entry, which is sorted by destination address.

Using the Statistics Group

This section describes how to use the Statistics group. It contains the following sections:

- Controlling the Statistics Group
- Viewing Statistics Group Data

Controlling the Statistics Group

This section describes how to configure the Statistics group.

Enabling Statistics Group Monitoring

At startup, the RMON agent adds an entry to each of the Statistics group control tables (MAC Layer and Promiscuous) so that statistics monitoring begins immediately. These control table entries are owned by the *monitor*. If a control table entry is deleted, you can enable monitoring by adding a new control table entry as described below.

To enable Statistics group monitoring, use the following commands:

SET RMON STATISTICS MAC_LAYER INTERFACE

SET RMON STATISTICS PROMISCUOUS INTERFACE

For example:

```
8250> set rmon statistics mac_layer interface
Entry created.
8250> set rmon statistics promiscuous interface
Entry created.
```

Viewing the Statistics Group Control Tables

To view lists of Statistics group control table entries, use the following commands:

SHOW RMON STATISTICS MAC_LAYER CONTROL ALL

SHOW RMON STATISTICS PROMISCUOUS CONTROL ALL

For example:

```
8250> show rmon statistics mac_layer control all

RMON Token Ring Mac Layer Statistics Control Table:

Index  Data Source                      Owner
-----  -----------                      -----
   1   interface                       system
```

Disabling Statistics Group Monitoring

To disable Statistics group monitoring, use the following commands:

CLEAR RMON STATISTICS MAC_LAYER

CLEAR RMON STATISTICS PROMISCUOUS

For example:

```
8250> clear rmon statistics mac_layer all
Entry cleared.
8250> clear rmon statistics promiscuous all
Entry cleared.
```

Viewing Statistics Group Data

To view data collected for all MAC addresses, use the following commands:

SHOW RMON STATISTICS MAC_LAYER DATA ALL

SHOW RMON STATISTICS PROMISCUOUS DATA ALL

SHOW RMON DISTRIBUTION PROMISCUOUS DATA ALL

For example:

```
8250> show rmon statistics mac_layer data all

RMON Token Ring Mac Layer Statistics:

Index : 1
Drop Events                     : 0
Octets                          : 24044
Packets                         : 89
Ring Purge Events               : 0
Ring Purge Packets              : 0
Beacon Events                   : 0
Beacon Time                     : 0
Beacon Packets                  : 0
Claim Token Events              : 0
Claim Token Packets             : 0
NAUN Changes                    : 0
Line Errors                     : 0
Internal Errors                 : 0
Burst Errors                    : 0
AC Errors                       : 0
Abort Errors                    : 0
Lost Frame Errors               : 0
Congestion Errors               : 0
Frame Copied Errors             : 0
Frequency Errors                : 0
Token Errors                    : 0
Soft Error Reports              : 0
Ring Poll Events                : 0


8250> show rmon statistics promiscuous data all

RMON Token Ring Statistics:

Index : 1
Drop Events                     : 0
Octets                          : 2948490
Packets                         : 21896
Broadcast Packets               : 6103
Multicast Packets               : 0
```

```
8250> show rmon distribution promiscuous data all

RMON Token Ring Distribution:

Distribution for index 1:

                    0%         25%       50%        75%        100%

Packet Size         |           |         |          |          |  Packets

-------------------------------------------------------------------------------

18   to 63          | *********                                  | 10903
64   to 127         | ************************                   | 27837
128  to 255         |                                            | 288
256  to 511         | ****                                       | 4663
512  to 1023        |                                            | 690
1024 to 2047        |                                            | 0
2048 to 4095        |                                            | 0
4096 to 8191        |                                            | 0
8192 to 18000       |                                            | 0
Greater Than 18000  |                                            | 0
```

Using the Source Routing Group

This section describes how to use the Source Routing group. It contains the following sections:

- Controlling the Source Routing Group
- Viewing Source Routing Group Data

Controlling the Source Routing Group

This section describes how to configure the Source Routing group.

Enabling Source Routing Group Monitoring

At startup, the RMON agent adds an entry to the Source Routing group control table so that Source Routing monitoring begins immediately. This control table entry is owned by the *monitor*. If this control table entry is deleted, you can enable Source Routing monitoring by adding a new control table entry using the following command:

SET RMON STATISTICS SOURCEROUTING INTERFACE

For example:

```
8250> set rmon statistics sourcerouting interface

Entry created.
```

Viewing the Source Routing Group Control Table

To view a list of Source Routing group control table entries, use the following command:

SHOW RMON STATISTICS SOURCEROUTING CONTROL ALL

For example:

```
8250> show rmon statistics sourcerouting control all
RMON Token Ring Source Routing Statistics Control Table:
IfIndex  Data Source                      Owner
-----    -----------                      -----
   1     interface                        system
```

Disabling Source Routing Group Monitoring

To disable Source Routing monitoring, use the following command:

CLEAR RMON STATISTICS SOURCEROUTING

For example:

```
8250> clear rmon statistics sourcerouting all
Entry cleared.
```

Viewing Source Routing Group Data

To view Source Routing group data, use the following command:

SHOW RMON STATISTICS SOURCEROUTING DATA ALL

For example:

```
8250> show rmon statistics sourcerouting data all

RMON Token Ring Source Routing Statistics:
Ring Number                     : 1
In Frames                       : 0
Out Frames                      : 0
Through Frames                  : 0
All Routes Broadcast Frames     : 0
Single Routes Broadcast Frames  : 4
In Octets                       : 0
Out Octets                      : 0
Through Octets                  : 0
All Routes Broadcast Octets     : 0
Single Routes Broadcast Octets  : 460
Local LLC Frames                : 1953
1 Hop Frames                    : 0
2 Hop Frames                    : 0
3 Hop Frames                    : 0
4 Hop Frames                    : 0
5 Hop Frames                    : 0
6 Hop Frames                    : 0
7 Hop Frames                    : 0
8 Hop Frames                    : 0
More Than 8 Hops Frames         : 0
```

Using the Token Ring Ring-Station Group

This section describes how to use the Token Ring Ring-Station and Token Ring Ring-Station Order groups. It contains the following sections:

- Controlling the Token Ring Ring-Station Group
- Viewing Token Ring Ring-Station Group Data

Controlling the Token Ring Ring-Station Group

This section describes how to configure the Token Ring Ring-Station group.

Enabling Token Ring Ring-Station Group Monitoring

At startup, the RMON agent adds an entry to the Token Ring Ring-Station group control table so that Token Ring Ring-Station monitoring begins immediately. This control table entry is owned by *monitor*. If this control table entry is deleted, you can enable Token Ring Ring-Station monitoring by adding a new control table entry using the following command:

SET RMON RINGSTATION INTERFACE

For example:

```
8250> set rmon ringstation interface
Entry created.
```

This command also enables the Token Ring Ring-Station Order group.

Viewing the Token Ring Ring-Station Group Control Table

To view a list of Token Ring Ring-Station group control table entries, use the following command:

SHOW RMON RINGSTATION CONTROL ALL

For example:

```
8250> show rmon ringstation control all

RMON Ring Station Control Table:

Index                          : 1
Table Size                     : 6
Active Stations                : 6
Ring State                     : 1
Beacon Sender                  : 00-00-00-00-00-00
Beacon NAUN                    : 00-00-00-00-00-00
Active Monitor                 : 10-00-5a-7a-a6-b3
Order Changes                  : 1
Owner                          : monitor
```

Disabling Token Ring Ring-Station Group Monitoring

To disable Token Ring Ring-Station monitoring, use the following command:

CLEAR RMON RINGSTATION 1

For example:

```
8250> clear rmon ringstation 1
Entry cleared.
```

This command also disables the Token Ring Ring-Station Order group.

Viewing Token Ring Ring-Station Group Data

To view Token Ring Ring-Station Group data, use the following commands:

SHOW RMON RINGSTATION DATA 1 ALL

SHOW RMON RINGSTATION DATA 1 HOST_ADDRESS *mac_address*

SHOW RMON RINGSTATION DATA 1 ORDER

For example:

```
8250> show rmon ringstation data 1 all
RMON Ring Station Group:

Index                          : 1
Mac Address                    : 00-00-00-00-10-40
Last NAUN                      : 12-00-4a-7a-a6-b3
Station Status                 : 2
Last Enter Time                : 27 Mar 96 14:43:22
```

```
Last Exit Time                  : 27 Mar 96 14:43:22
Duplicate Address               : 0
In Line Errors                  : 0
Out Line Errors                 : 0
Internal Errors                 : 0
In Burst Errors                 : 0
Out Burst Errors                : 0
AC Errors                       : 0
Abort Errors                    : 0
Lost Frame Errors               : 0
Congestion Errors               : 0
Frame Copied Errors             : 0
Frequency Errors                : 0
Token Errors                    : 0
In Beacon Errors                : 0
Out Beacon Errors               : 0
Insertions                      : 0

[Output repeats for each Mac address]


8250> show rmon ringstation data 1 host_address 18-40-00-00-30-80

RMON Ring Station Group:

IfIndex                         : 1
Mac Address                     : 18-40-00-00-30-80
Last NAUN                       : 12-00-4a-7a-a6-b3
Station Status                  : 2
Last Enter Time                 : 27 Mar 96 14:43:21
Last Exit Time                  : 27 Mar 96 14:43:21
Duplicate Address               : 0
In Line Errors                  : 0
Out Line Errors                 : 0
Internal Errors                 : 0
In Burst Errors                 : 0
Out Burst Errors                : 0
AC Errors                       : 0
Abort Errors                    : 0
Lost Frame Errors               : 0
Congestion Errors               : 0
Frame Copied Errors             : 0
Frequency Errors                : 0
Token Errors                    : 0
In Beacon Errors                : 0
Out Beacon Errors               : 0
Insertions                      : 0
```

```
8250> show rmon ringstation data 1 order
RMON Ring Station Order:

IfIndex                         : 1
Order Index                     : 1
Mac Address                     : 10-00-f1-0f-3b-5d


IfIndex                         : 1
Order Index                     : 2
Mac Address                     : 00-00-30-80-ef-b3


End of Table
```

Using the Alarm and Event Groups

RMON defines alarm and event functions in which user-defined alarms trigger event actions. An alarm is generated when a statistical value crosses a user-defined threshold. The alarm triggers a user-selected event action.

This section contains the following sections:

- Alarm Thresholds Overview
- Setting Up Alarms and Events

Alarm Thresholds Overview

This section describes how thresholds work. It contains the following sections:

- Rising and Falling Thresholds
- Re-arming Alarm Thresholds
- Initial Trigger
- Sample Intervals
- Delta and Absolute Values

Rising and Falling Thresholds

RMON defines two types of thresholds: *rising* and *falling*. Figure 6-2 shows an example of how rising and falling thresholds work.

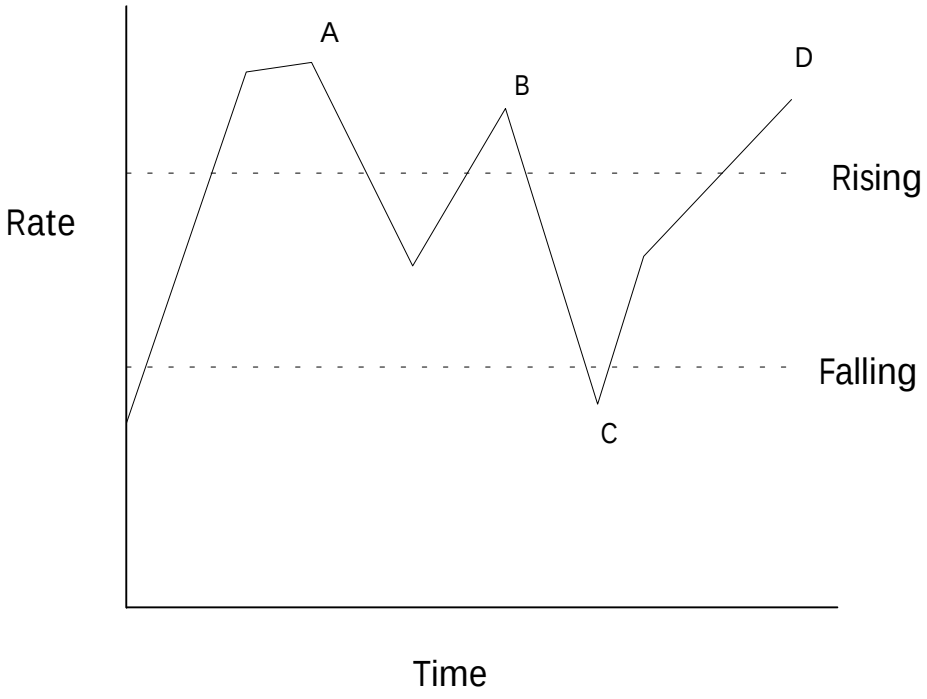


Figure 6-2. Rising and Falling Alarm Thresholds

The two dotted lines represent the rising and falling thresholds. The rising threshold triggers an alarm when the rate exceeds the rising threshold. The falling threshold triggers an alarm when the statistic value drops below the falling threshold.

Re-arming Alarm Thresholds

In Figure 6-2, the rising threshold triggers an alarm at points A and D. The rising threshold does not generate an event at point B because the alarm is

not *re-armed* until the rate drops below the falling threshold. Once the rate drops below the falling threshold (at point C), the rising threshold is re-armed.

Similarly, once a falling threshold alarm occurs, the falling threshold is not re-armed until the rate again exceeds the rising threshold. Re-arming prevents repeated alarms caused by a rate fluctuating just above and below the threshold.

Initial Trigger

The *initial trigger* defines whether the rising and falling thresholds are armed when monitoring begins. You can arm:

- Rising threshold only
- Falling threshold only
- Both rising and falling thresholds

Sample Intervals

When setting up an alarm, you define a *sample interval*. The sample interval is how often the RMON probe compares the statistic to the threshold. If you define a sample interval of 1 minute, the RMON probe compares the statistic to the threshold once per minute.

Delta and Absolute Values

You can define a threshold to test delta or absolute values.

- A *delta value* is the change in the value since the last sample. For example, suppose you are defining thresholds for a packet counter. If the value at one sample point is 32,700, and the value at the next sample point is 33,420, the delta value is 33,420 – 32,700 = 720. A delta value defines a rate, where the rate is the change in the counter value for each sample interval. Delta values are typically used to monitor the counter rates.

- An *absolute value* is the value of the statistic at the sample point. For example, if the value at one sample point is 32,700, the absolute value is 32,700. Absolute values are typically used to measure statistics defined as integers or gauges.

Setting Up Alarms and Events

This section describes how to set up alarms and events. It contains the following sections:

- General Procedure for Setting Up Alarms and Events
- Configuring Events
- Clearing Events
- Showing Events
- Configuring Alarms
- Clearing Alarms
- Showing Alarms
- Example: Configuring Alarms and Events

General Procedure for Setting Up Alarms and Events

To set up alarms and events:

1. Configure which events occur when the alarm thresholds are crossed.
2. Configure alarm thresholds to trigger the event.

Configuring Events

You can configure up to 30 events. To configure an event, use the following command:

SET RMON EVENT *event_type community*

Where:

- *event_type* is *log*, *trap*, *log_trap*, or *none*
- *community* is the SNMP community to receive a trap, if defined. Use the SHOW COMMUNITY command to list SNMP community names.

For example:

```
8250> set rmon event trap NCS

Enter one line for event description:
> RingPurgePackets Alarm: >5 per hour!!
Entry 3 created.
```

Clearing Events

To clear an event from the control table, use the following command:

CLEAR RMON EVENT *control_index*

Where:

- *control_index* is the number of the event in the control table. You can specify all to clear all events.

For example:

```
8250> clear rmon event 3

Entry 3 cleared.
```

Showing Events

To view a list of control table entries, use the SHOW RMON EVENT CONTROL ALL command.

For example:

```
8250> show rmon event control all

RMON Event Control Information:

Index Type             Community        Time Since Sent     Owner
----- ---------------- ---------------- ------------------- ------

    1 Log              (None)           Not Triggered       monitor

Description: Internal log events

    2 Log and Trap     traps            Not Triggered       monitor

Description: MIB II events

    3 Log              public           Not Triggered       system

Description: RingPurgePackets Alarm: >30 per hour!!

    4 None             public           Not Triggered       system

Description: Re-arming RingPurgePackets alarm.
```

Note: The entries owned by *monitor* are created by the RMON probe at startup.

Configuring Alarms

You can configure up to 15 alarms.

To configure an alarm to trigger an event, use the following command:

SET RMON ALARM *stat_group stat_type.interface* RISING *threshold event* FALLING *threshold event time trigger alarm type*

For an example of how to build a SET RMON ALARM command, refer to the section Example: Configuring Alarms and Events on page -36.

Clearing Alarms

To clear (remove) one or all of the alarms from the control table, use the following command:

CLEAR RMON ALARM *control_index*

Where:

- *control_index* is the number of the task in the control table.

For example:

```
8250> clear rmon alarm 1
Entry cleared.
```

Showing Alarms

To view a list of alarm control table entries, use the SHOW RMON ALARM CONTROL ALL command.

For example:

```
8250> show rmon alarm control all

RMON Alarm Control Information:

Index Interval            Sample Type Owner
----- ------------------- ----------- ----------------
    1 0 day(s) 01:00:00   Delta       system

Monitored Variable              : TokenRingMLStatsRingPurgePackets.1
Current Value                   : 0
Rising  Threshold / Event       : 5 / 3
Falling Threshold  /  Event     : 0 / 4
```

Example: Configuring Alarms and Events

The following example configures an alarm that triggers a trap when the RMON probe records more than 30 RingPurgePackets in an hour. The first time the alarm occurs, it triggers the trap event, then does not trigger another trap event until the alarm condition occurs a second time.

To configure the alarm and events for this example:

1. Configure the trap event to be triggered by the rising threshold alarm:

```
8250> set rmon event trap

Enter one line for event description:
>RingPurgePackets Alarm: >30 per hour!!
Entry 3 created.
```

2. Configure an event of event_type none to re-arm the rising threshold alarm when the falling threshold alarm occurs:

```
8250> set rmon event none

Enter one line for event description:
>Re-arming the RingPurgePackets alarm.
Entry 4 created.
```

3. To verify event entries, use the SHOW RMON EVENT CONTROL ALL command:

```
8250> show rmon event control all

RMON Event Control Information:

Index Type             Community        Time Since Sent     Owner

----- ---------------- ---------------- ------------------- ---------
    1 Log              (None)           Not Triggered       monitor

Description: Internal log events

    2 Log and Trap     traps            Not Triggered       monitor

Description: MIB II events

    3 Log              public           Not Triggered       system

Description: RingPurgePackets Alarm: >30 per hour!!

    4 None             public           Not Triggered       system

Description: Re-arming RingPurgePackets alarm.
```

4. To create the alarm that triggers these events, build the SET RMON ALARM command as follows:

   a. `set rmon alarm token_ring_mlstats RingPurgePackets.1`

      token_ring_mlstats RingPurgePackets.1 defines RingPurgePackets as the statistic to test. For the 8250 Token Ring Module, the interface is always .1.

   b. `set rmon alarm token_ring_mlstats RingPurgePackets.1` **`rising 30 3`**

      The rising threshold of 30 (30 RingPurgePackets) triggers event number 3.

   c. `set rmon alarm token_ring_mlstats RingPurgePackets.1 rising 30 3` **`falling 1 4`**

      The falling threshold 1 (one or fewer RingPurgePackets) causes event 4. Event 4's event type is none. Its purpose is to re-arm the rising alarm.

   d. `set rmon alarm token_ring_mlstats RingPurgePackets.1 rising 30 3 falling 1 4` **`01:00`**

      The sample interval (hh:mm) is 1 hour (01:00)

   e. `set rmon alarm token_ring_mlstats RingPurgePackets.1 rising 30 3 falling 1 4 01:00` **`rising_start`**

      The initial trigger condition is rising_start, which arms the rising threshold alarm only.

   f. `set rmon alarm token_ring_mlstats RingPurgePackets.1 rising 30 3 falling 1 4 01:00 rising_start` **`delta_type`**

      The alarm evaluates delta values. This defines the threshold as a rate (30 RingPurgePackets per hour).

Interpreting Token Ring Statistics

This section describes Token Ring error statistics tracked by several of the Token Ring statistics groups. It contains the following sections:

- Soft Errors
- Hard Errors
- Insertion Errors

Soft Errors

Soft errors are minor errors that typically do not require intervention by the network administrator. The Token Ring protocol uses simple ring recovery procedures to correct problems caused by soft errors. Excessive soft errors can degrade the performance of the network, so be sure to monitor soft error levels and understand the possible causes.

Ring stations monitor their own activity for errors, and check received frames for errors. They report detected errors to the REM (Ring Error Monitor) in error report frames. The RMON probe also receives error report frames and uses them as its source for soft error counts.

Soft errors are of two types:

- *Isolating errors* point to a specific station or cable on the network as the error source.
- *Non-isolating errors* do not point to a specific error source.

Table 6-2 defines isolating errors and describes possible causes.

Table 6-2. Isolating Errors

Error	Definition	Possible Cause	Corrective Action
Internal Error	Recoverable error occurring within the reporting station's NIC (Network Interface Card).	Excessive Internal Errors indicate marginal NIC operation.	Verify that the NIC is operating properly. Replace if necessary.
Burst Error	The reporting station detected a bad signal of short duration while receiving from its NAUN (Nearest Active Upstream Neighbor).	Typically due to stations entering or leaving the ring, in which case a similar number of ring reconfigurations (recorded as Order Changes under Ring Station Control Statistics) occur.	No action.
		Excessive burst errors in the absence of ring reconfigurations indicate: • A possible problem with the lobe cable of the reporting station • A possible problem with the reporting station's NAUN.	Verify that the: • Lobe cable of the reporting station is properly connected and is not defective. • NAUN is operating properly. Replace if necessary.

Table 6-2. Isolating Errors (Continued)

Error	Definition	Possible Cause	Corrective Action
Line Error	The reporting station detected an FCS (Frame Check Sequence), or less often, a Manchester code violation, in a received frame.	Typically related to ring recovery or ring reconfiguration, but may indicate a problem with the reporting station's NAUN.	Verify that the NAUN is operating properly. Replace if necessary.
Abort Error	The reporting station's NIC was forced to transmit an Abort Delimiter frame due to a recoverable internal error.	Excessive Abort Errors indicate marginal NIC operation.	Verify that the NIC is operating properly. Replace if necessary.
AC Error	The reporting station received more than one AMP (Active Monitor Present) or SMP (Standby Monitor Present) frame with the A (Address Recognized) and C (Frame Copied) bits equal to zero, without first receiving an intervening AMP frame.	Excessive AC Errors indicate a possible problem with the reporting station's NAUN.	Verify that the NAUN is operating properly. Replace if necessary.

Table 6-3 defines non-isolating errors and describes possible causes and corrective action.

Table 6-3. Non-Isolating Errors

Error	Definition	Possible Cause	Corrective Action
Lost Frame Error	The reporting station sent a frame but did not receive it back.	Interference or corruption.	No action.
Congestion Error	The reporting station could not receive a frame addressed to it.	Usually occurs because the station's NIC lacks the buffer space to handle incoming traffic. This is due to one of the following: • A faulty or misconfigured NIC • A station or software application sending excessive traffic to this station.	Verify that: • The NIC is configured correctly and is operating properly. Reconfigure or replace, as necessary. • No software applications are causing excessive traffic on the network.
Frame Copied Error	The reporting station received a frame addressed to it, but with one or both of the A bits set to 1.	May indicate the presence of a station with a duplicate address.	Determine if more than one station has the same address.

Table 6-3. Non-Isolating Errors (Continued)

Error	Definition	Possible Cause	Corrective Action
Frequency Error	The incoming signal frequency differs significantly from the expected frequency.	Excessive errors may indicate: • A configuration problem (a station is incorrectly set to the wrong ring speed) • A problem with the Active Monitor, which controls the master clock • A problem with the NAUN.	Fix problems listed in Possible Cause.
Token Error	The Active Monitor determined that the token was lost.	Interference or corruption.	No action.

Hard Errors

Hard errors are serious errors that require a network component be bypassed for the ring to resume normal operation. The ring can recover dynamically from some hard errors, but others require intervention by the network administrator.

When a hard error occurs, the station detecting the error issues a beacon frame. A beacon frame indicates that the problem lies with one of the following:

- Station sending the beacon frame
- NAUN of the station sending the beacon frame
- Lobe cables separating these two stations

The Token Ring Ring-Station Group maintains counts of In Beacon Errors (beacon frames received) and Out Beacon Errors (beacon frames transmitted) for each station.

Insertion Errors

The Ring Station Group keeps track of the number of times each station inserts itself into the ring. Excessive insertions may indicate a problem with the station or its NIC.

Chapter 7. Troubleshooting

This chapter provides help in isolating and correcting problems that may arise during the installation process, or during normal operation of the 8250 Token Ring Management Module (TRMM). This chapter contains the following sections:

- Troubleshooting Power Problems
- Troubleshooting Using TRMM LEDs
- Troubleshooting Terminal Interface Problems
- TRMM Network Impact
- TRMM Trap Messages

If a LED does not light as expected, press the LED check button on the Controller Module to verify that the LED is not burned out. If the LED is functional, refer to the troubleshooting tables within this chapter. The LED check is presented here rather than being repeated for each LED.

Troubleshooting Power Problems

Under normal conditions, when you install the TRMM, the Status LED lights and the Master Mgt LED lights briefly. The Master Mgt LED remains on if the TRMM is elected master. Table 7-1 lists some of the common problems that may arise when installing your TRMM.

Table 7-1. Applying Power Suggestions

Problem	Troubleshooting Suggestions
Power is on, but the Status LED does not light.	Verify that the TRMM is installed correctly by following the installation instructions in Chapter 3.
	Press the Reset button on the TRMM.
	Try the TRMM in another slot in the hub.
	If the LED still does not light, the software on the Flash EPROM may be corrupted. Try downloading a new copy of the software. If downloading software does not solve the problem, call your supplier for assistance.
Master Mgt LED not lit.	If there is more than one TRMM in the hub, verify that only one TRMM is set to a mastership priority of 10 (using the SHOW MODULE VERBOSE command). Then press the Reset button on the TRMM to force an election. You can also issue the RESET DEVICE command to reset the module.
	Check if another management module (TRMM or EMM) in the hub is master.
	Try the suggestions for the previous problem.

Troubleshooting Using TRMM LEDs

Table 7-2 describes how to troubleshoot network operations with the TRMM LEDs. The table also provides suggestions for correcting any problems that may occur.

Table 7-2. Troubleshooting With the TRMM LEDs

LED	LED Status	Possible Problem	Troubleshooting Suggestion
Master Mgt	OFF	TRMM is not master.	None.
	1 Blink	Election in progress.	None.
Download	LED remains lit longer than 20 minutes (this may occur if you perform the download at slower baud rates.)	Download failed.	Press Reset button to reset module and try download again.
BAS (Basic)	OFF	TRMM is Advanced version.	None.
BCN	On	LED remains lit.	Possible defective module or ring problem. Replace module, or segment the module from the ring.

Table 7-2. Troubleshooting With the TRMM LEDs (Continued)

LED	LED Status	Possible Problem	Troubleshooting Suggestion
RI and RO	OFF	Port is disabled.	Enable port.
		TRMM not powered.	Check the Controller Module Power LEDs.
		Faulty TRMM.	Replace module.
	1 Blink	No cable installed.	Install the cable or disable the port.
	2 Blinks	No stations on the ring.	Verify that the module is configured properly on the ring.
		Port is enabled but a squelch error is detected. This condition causes the signal to wrap.	Check for a faulty cable.
4M	OFF	Normal, unless TRMM is configured for 4 Mbps operation.	Press LED check button on the Controller Module.
Status	OFF	Possible defective module.	Replace module.
Backup	OFF	TRMM is master.	None.
	On	TRMM is slave.	None.

Table 7-2. Troubleshooting With the TRMM LEDs (Continued)

LED	LED Status	Possible Problem	Troubleshooting Suggestion
ADV (Advanced)	OFF	TRMM is Basic version.	None.
16M	OFF	Normal, unless TRMM is configured for 16 Mbps operation.	Press LED check button on the Controller Module.

Troubleshooting Terminal Interface Problems

Table 7-3 lists some common problems that may occur when you try to have the TRMM communicate with a terminal. If necessary, refer to the directions in Chapter 3 for instructions on attaching your terminal to the TRMM using the RS-232 serial port connector.

Table 7-3. TRMM Terminal Interface Suggestions

Problem	Troubleshooting Suggestions
Nothing appears on the screen.	Make sure the RS-232 cable meets the specifications detailed in Chapter 3.
	Make sure the RS-232 cable is securely connected to both devices. See Chapter 3 for installation instructions.
	Verify that the baud rates match for the terminal and the TRMM.
Characters appear on the screen, but are garbled.	Verify that the TRMM and the terminal settings match for baud, data bits, stop bits, and parity. These values are explained in Chapter 3 and Chapter 4.
The SET command does not work.	Make sure you are signed on as the Administrator or super user and that you are connected to the master TRMM.
Abbreviated input is used and pressing Space does not complete the input.	Enter enough characters for the TRMM to distinguish between different commands and options.
Random characters are lost.	Set the flow control on the terminal to XON/XOFF.
Characters are lost when connected to the TRMM through a modem.	Make sure the STOP_BITS value on the terminal is set to 1 STOP_BITS.

Table 7-3. TRMM Terminal Interface Suggestions (Continued)

Problem	Troubleshooting Suggestions
The management prompt on the screen is not as you set it.	You may be connected to a remote device. Refer to the TELNET and LOGOUT command descriptions (Chapter 4).
Power up (switchover) brings up a different configuration than the one last set.	Make sure you save your configuration changes.
You are not receiving any statistics from the hub.	Check that the TRMM and the modules in the hub are not isolated.
The Master Mgt Module LED blinks sporadically.	Check for multiple TRMMs, and verify that only one has been set to a mastership level of 10.
The >> prompt appears on the screen.	The TRMM is running in maintenance mode. Enter the BOOT command to return to management mode and the 8250> prompt.

TRMM Network Impact

This section describes the impact of the TRMM on the network. It is designed to help the network administrator identify the source of packets on the network. Specifically, this section helps identify 8250 System Concentrator-generated packets.

The TRMM generates packets on the network (channel) in the following instances:

- When establishing and maintaining a TELNET session, either as a client or a server.
- When translating an IP address to a MAC address using the Address Resolution Protocol (ARP).
- When initiating or responding to a PING command.
- When responding to an SNMP command.
- When sending SNMP alerts to a workstation.
- When conforming to the IEEE 802.5 MAC protocol. For example, sending active monitor or standby monitor packets and sending informational packets to the Ring Error Monitor functional address.
- When performing an in-band download using TFTP.

In all other cases, the TRMM does not generate any network activity. Traffic statistics are collected by operating in promiscuous mode, that is, listening to each packet on the network. Other modules in the hub are managed using a separate control bus on the 8250 backplane.

TRMM Trap Messages

A trap message is sent to the console when a change is made or an error occurs in a hub that has an installed TRMM. The trap is also sent to the designated trap receiver (for example, management workstation) if you have entered this information in the TRMM community table. For example, if a module is removed from a hub, a message that describes the change is sent to the console, as shown below:

```
Message received from this device on 15:53 Tue 16 Jan 96:

Enterprise:    IBM

Enterprise Specific Trap:    Slot Down

Message Information:
        Slot Number:   6
Module Type Number:    6
Module Description:    T20MS-RJ45S
```

The first two fields in the trap message are described in Table 7-4. The remainder of the fields are specific to the type of trap received and are self-explanatory.

Table 7-4. TRMM Trap Message Fields

Field	Description
Enterprise	Describes the enterprise (organization) responsible for this type of trap message.
Enterprise Specific Trap	One of the following trap messages: Slot Up or Slot Down Port Up or Port Down Trunk Up or Trunk Down Fatal Error Environment Change Threshold Exceeded

SNMP traps are also sent to the TRMM console when they occur. An example of an SNMP trap would be when a device attempts to gather information (read) from the TRMM, but the address of the device has not been added to the community table with that access level. The message that would appear in this instance is shown below:

```
Message received from this device on 15:53 Tue 16 Jan 96:

Enterprise:    IBM

SNMP Generic Trap:    SNMP Authentication Failure
```

Chapter 8. Downloading TRMM Firmware

This chapter describes download procedures for loading new software to the Flash or Boot EPROM in your TRMM.

The IBM Universal Code Download Kit (UCDK) is used to install and configure the ProComm** software on your Personal Computer. The ProComm software enables your PC to communicate with the TRMM, using the module's RS-232 port.

You can download software in either of two ways:

- **In-band** (Recommended) — Downloads the software from a file stored on a file server.
- **Out-of-band** — Requires that your terminal be connected directly to the module's RS-232 port.

This chapter contains the following sections:

- Download Requirements
- In-band Download Instructions
- Understanding the Universal Code Download Kit and UDK Processes
- Out-of-Band Download Instructions

Download Requirements

This section contains the following sections:

- Important Prerequisites to the Download Procedure
- Items Required to Complete the Download Procedure

Important Prerequisites to the Download Procedure

You must meet the following requirements before beginning the download procedure:

1. Ensure that the TRMM has an installed 2 MB SIMM component.

   The 1 MB SIMM does not provide the memory capacity for the TRMM Version v4.0 software. To determine the type of SIMM currently installed on your TRMM, use the SHOW DEVICE command to display the DRAM KB value.

   - 1024 KB value indicates a 1 MB SIMM.
   - 2048 KB value indicates a 2 MB SIMM.

   To update the SIMM on your TRMM, contact your IBM representative and order the TRMM 2 MB SIMM Upgrade Kit.

2. If you are using an in-band download, ensure the module has Version v2.10 or later software installed on the Flash EPROM. (If you are using an out-of-band download, you do not need to upgrade the TRMM Version v2.10 software prior to downloading Version v4.0 software.) To display the TRMM software version, use the SHOW DEVICE command. If the Flash EPROM is not at Version v2.10 or later, perform the download of the Version v2.10 software located on the Version v4.0 diskette.

3. Verify the data integrity of the module by issuing the following SHOW commands:
   - SHOW GROUP
   - SHOW SCHEDULES
   - SHOW COMMUNITY
   - SHOW DEVICE
   - SHOW BOOTP
   - SHOW SCRIPT
   - SHOW THRESHOLD
4. Familiarize yourself with the two-step download process for in-band download of Flash code. Execute the SHOW commands listed in step 3 after the first stage of the Flash download to verify module data integrity.

Note: Always update boot code, if necessary, prior to downloading flash code.

Items Required to Complete the Download Procedure

You must have the following items to complete the download procedure:

- The IBM Universal Code Download Kit (Part Number 80G3150, Feature Code 3150). This is required for out-of-band downloads only. The Universal Code Download Kit includes:
  - *ProComm Reference Manual* (from DATASTORM** TECHNOLOGIES, INC..)
    shrink-wrapped with:
    - ProComm** diskettes (3½-inch disks)
    - ProComm software license.
  - IBM diskettes (3½-inch disks)
  - 10 ft. RS-232 cable
  - 25-pin to 9-pin adapter.
- 8250 Token Ring Management Module upgrade kit from IBM, including:
  - IBM diskettes, 3½-inch disks (two sets for site license)
  - IBM software license
  - IBM Customer Registration Card - must be returned for notification of future software enhancements
  - Software Release Notes.
- IBM personal computer or UNIX® workstation capable of mounting a DOS-formatted high-density diskette, and a hard drive, or two high-density diskette drives.
- 640 K of available RAM (if using a PC).

Warning: A personal computer used to download the new software must not be running any background RAM processes, such as electronic mail systems, because they will interfere with the download procedure.

Note: If a download fails *while downloading* the Flash EPROMs, the TRMM may not be able to boot successfully. The programming of the Flash EPROMs occurs during an *in-band* download after the message Download Successful....Programming Devices....Please Wait displays.

The programming of Flash EPROMs occurs during an *out-of-band* download after the message Transfer Complete displays. This failure is indicated by the Download LED remaining lit for more than 2 minutes after the message displays or all of the LEDs remaining lit after a reset. If this failure occurs, contact Customer Support for instructions.

In-band Download Instructions

The TRMM provides an in-band download feature that allows you to update your TRMM Flash or Boot EPROMs using TFTP (Trivial File Transfer Protocol). TFTP allows the transfer of files to and from a remote machine. By using the TFTP protocol, you can in-band download new software to a TRMM from a remote network server.

Warning: The files must be downloaded in the proper order or the TRMM may fail.

Warning: You cannot revert from TRMM Version v4.0 or later to TRMM Version v3.3 or earlier.

The following prerequisites must be completed prior to initializing the download:

- You must have a TFTP server on the network to perform in-band downloads (for example, an IBM workstation).
- TRMMs to be updated must be assigned to a network that can reach the TFTP server.

Downloading Files on UNIX Systems

A TRMM UDK diskette contains up to three files, which must be downloaded in the following order:

1. **trmBvxxx.bin**, which updates the Boot EPROM
2. **trmFdxxx.bin**, which contains the preliminary download code
3. **trmFvxxx.bin**, which completes the Flash EPROM upgrade

The following procedure is an example of loading files on a Sun™ platform. Your commands may vary depending on the UNIX version you use.

Note: Before you start, make sure you have at least 4 MB of hard drive or server space to contain the files.

To load the files on a UNIX system:

1. Place the first 3Com TRMM UDK diskette in the floppy drive.
2. At the UNIX prompt, issue the following command to mount the DOS diskette:

   ```
   mount /pcfs
   ```

   For this command to work, the standard /pcfs mount must be specified in /etc/fstab.
3. Change to a directory that has enough available space to contain the contents of the two diskettes. For example, change to the user home directory ($HOME).
4. Create a directory for the files using the following command:

   ```
   mkdir trmm40
   ```
5. Copy the files on the diskette to the new directory:

   ```
   cp /pcfs/*.* /$HOME/trmm40/
   ```

   Copying takes a few minutes.
6. Change back to the user home directory:

   ```
   cd /$HOME/trmm40
   ```
7. Verify that the file copied successfully:

   ```
   ls -la
   ```
8. Unmount (dismount) the diskette:

   ```
   umount /pcfs
   ```
9. Eject the 3Com UDK diskette:

   ```
   eject
   ```

Initiating the Download

To perform an in-band download:

Warning: Starting with TRMM Version v4.0, there are three files that you must download to the TRMM. If you fail to download all three files, in the recommended sequence, your TRMM will not function properly.

1. From your UNIX workstation, connect to the TRMM you want to download to using the TELNET command. For example:

   ```
   csh> telnet trmm_4
   ```

Note: If your TFTP server is running on a Sun system, the server looks for the appropriate .BIN file in the `/tftpboot` directory. If your server is running in a DOS environment, the personal computer must be in the directory that contains the .BIN file when you start the server.

2. If the connection is successful, log in to the TRMM.
3. Configure the TFTP parameters by issuing the following management commands.

Step	TFTP Commands
1 (boot)	8250> **set tftp file_name trmBv*xxx*.bin** 8250> **set tftp file_type boot** 8250> **set tftp server_ip_address *x.x.x.x***
2 (flash, part 1)	8250> **set tftp file_name trmFd*xxx*.bin** 8250> **set tftp file_type flash**
3 (flash, part 2)	8250> **set tftp file_name trmFv*xxx*.bin**

4. Issue the SHOW TFTP command to verify the TFTP parameters previously set.

```
8250> show tftp

—— TFTP Variables: ——

TFTP Server IP Address:   x.x.x.x
TFTP File Name:           trmbvxxx.bin
TFTP File Type:           boot
TFTP Result:
```

5. Issue the SAVE ALL command to save the TFTP parameters, as well as any unsaved TRMM configuration changes.

6. Issue the DOWNLOAD INBAND command to begin the download.

```
8250> download inband
WARNING: Download will erase your current operational code.
You will need the following to replace the software:
1. IBM Management Module Software residing on a TFTP
   server accessible over the network.
2. The TFTP variables (See SHOW TFTP and SET TFTP) must be
   configured for the TFTP server to be used for the download.
3. The serial number of the Upgrade Distribution Kit.

  Management Module's ID number: 1234
```

   The following message is then displayed:

```
If you are positive that you want to perform a network
download, enter the download in-band again within 10
seconds. Otherwise, the sequence will be aborted.
```

7. Press Ctrl-R to redisplay the previous command and press Enter to begin the download process. Once the download process begins, do not press any keys or otherwise interfere with the process. The download takes 15 to 30 seconds to complete.

```
8250> download inband
```

   When the download completes successfully, the following message is displayed and the TRMM boots up under the new code.

```
Download Successful....Programming Devices....Please Wait

Token Ring Management Module (vx.x)
Copyright (c) 199x IBM Corporation

Login: system

Password: old administrator password
```

```
Welcome to Super User service on 8250.
8250>
```

8. Repeat this procedure for each of the files in the UDK.

Note that this procedure must be followed for *each* TRMM to be updated. That is, after the first download is complete, you must log in to or establish a TELNET session with the next TRMM and again issue the TFTP commands to that TRMM.

You may also retry the download procedure. The TRMM retains the original code while the new code is being downloaded. Once the download process is complete, the TRMM verifies the integrity of the new code before copying it over the old code. If the download fails, the original code is still intact, allowing you to retry the download process.

Understanding the Universal Code Download Kit and UDK Processes

The IBM Universal Code Download Kit (UCDK) makes system upgrades fast and easy for all IBM products that are equipped with upgradable PROMs. You must purchase both the Universal Code Download Kit and the product UDK the first time you upgrade the software. All updates after that time require that you purchase only the new version of the UDK. You can re-use your original Universal Code Download Kit.

When IBM issues a software upgrade, the upgrade is sent on diskette (UDK) to all Automatic Update Service (AUS) customers. AUS is a feature for 8250 upgradable module.

Out-of-Band Download Instructions

Refer to the *IBM Universal Code Download Kit Installation Instructions* (80G3152) information on:

- Installing ProComm Software
- Setting Up ProComm (Line and Terminal Settings)
- Downloading the Microcode.

Appendix A. Specifications

This appendix lists the specifications for the Basic and Advanced versions of the 8250 Token Ring Management Module and Token Ring connector requirements. This appendix contains the following sections:

- General Specifications
- Electrical Specifications
- Environmental Specifications
- Mechanical Specifications
- Hardware Specifications
- Token Ring Connector Requirements

General Specifications

Model Numbers: Basic (Feature Code 3823)
Advanced (Feature Code 3884)

Data Rate: Switchable 4 Mbps or 16 Mbps (million bits per second)

Data modulation: Manchester

Backplane Interface: 96-pin edge connector, compatible with IBM 8250 Multiprotocol Intelligent Hubs.

Port Connector: RS-232 (DB-25)

Ring-In/Ring-Out Copper Ports

RJ-45 Connector

Electrical Specifications

Power Requirements:
+5 V ± 5%, +12 V ± 5%, -12 V ± 5%
3.5 Amp for +5 V, 0.06 Amp for +12 V, 0.03 Amp for -12 V

Fuse: 5.0 Amp Fast Blow for +5 V
0.5 Amp Fast Blow for +12 V
0.5 Amp Fast Blow for -12 V

Watts: 19 Watts

Environmental Specifications

Operating Temperature: 0 °C to 50 °C (32 °F to 122 °F)

Storage Temperature: -30 °C to 65 °C (-22 °F to 149 °F)

Humidity: less than 95%, non-condensing

BTU/hour: 64.8

Mechanical Specifications

TRMM Basic Dimensions: 1.0" W x 10.25" L x 8.5" H
(2.54 cm x 26.04 cm 21.6 cm)

TRMM Basic Weight: 1.25 lb. (.57 kg.)

TRMM Advanced Board Dimensions: .7" W x 5.4" L x 2.85" H
(1.78 cm x 13.7 cm x 7.24 cm)

TRMM Advanced Board Weight: .25 lb. (.11 kg.)

Hardware Specifications

Memory

256 KB Boot Flash EEPROM

1 MB Code Flash EEPROM

2 MB of DRAM

32 KB battery-backed SRAM

512 KB DRAM Token Ring Processor and Buffer

Internal Memory

256 bytes Instruction Cache (68EC030)

256 bytes Data Cache (68EC030)

2 KB SRAM (internal to 68302)

Special Circuits

Interface to upgrade for each MAC address

Token Ring network monitor

Real-Time Clock

Token Ring Connector Requirements

The IEEE 802.5 Token Ring standard for pinouts must be used. Token Ring uses 2 pairs of wire: pins 3 & 6 and pins 4 & 5. If the pairs are not configured this way, the connection will not work properly. An 8-pin connector on datagrade cable must have the following pin pairings:

- pins 4 and 5 are pair 1
- pins 3 and 6 are pair 2
- pins 1 and 2 are pair 3 (not used)
- pins 7 and 8 are pair 4 (not used)

Figure A-1 shows the correct pin pairings for an 8-pin Token Ring connector.

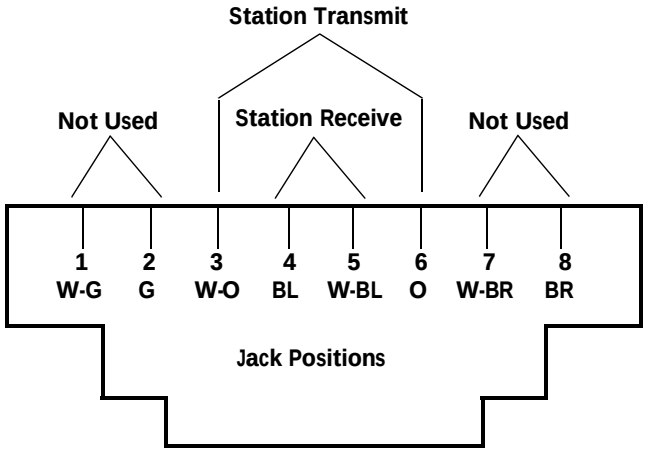


Figure A-1. Token Ring 8-Pin Connector

Note: Use only STP cabling to connect devices through the copper Ring-In/Ring-Out ports.

Appendix B. MIB Groups

This appendix describes the MIB-II and IBM MIB groups that are supported by the TRMM.

MIB-II Groups

The following MIB-II groups are supported in TRMM Version v4.00.

- - system
- - if
- - ip
- - icmp
- - udp
- - snmp
- - dot5
- RMON
  - rfc-1271
  - Token Ring Mac-layer Statistics Group
  - Token Ring Promiscuous Statistics Group
  - tokenRingMLStatsTable
  - tokenRingPStatsTable
  - rfc-1513

IBM MIBs

The following IBM MIB groups are supported in TRMM Version v4.00.

- - chipgen
- - chipEcho
- - olAgents
- - olConc
- - olEnv
- - olModules
- - olGroups
- - olNet
- - olTRnet
- - chipTTY
- - chipTFTP
- - chipAlert
- - chipBootP
- - olThresh

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W