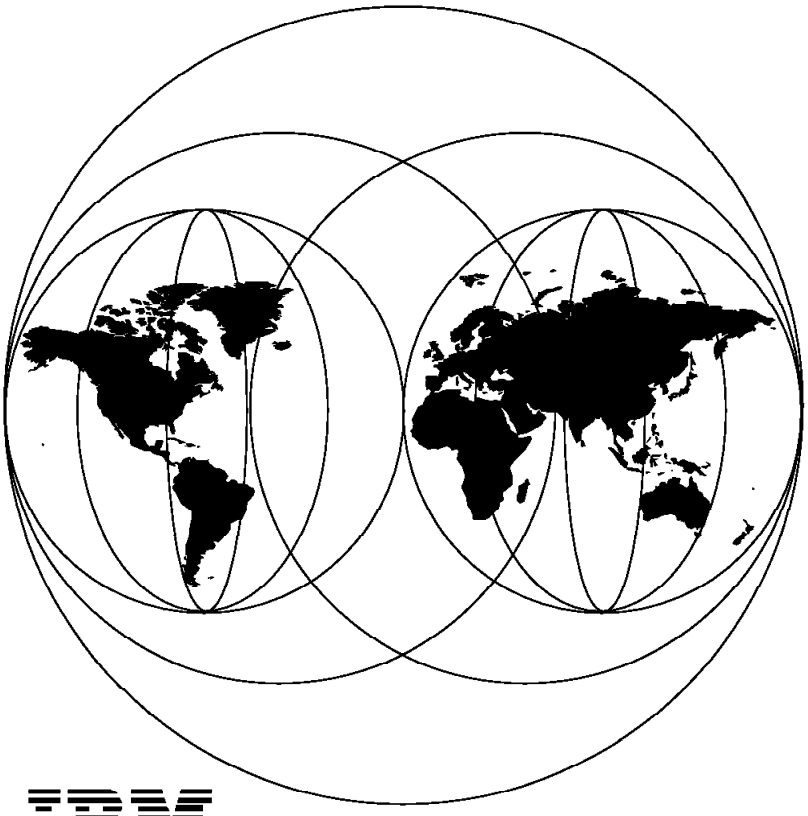
International Technical Support Organization

GG24-4370-00

8260 Multiprotocol Intelligent Switching Hub

May 1995



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

GG24-4370-00

8260 Multiprotocol Intelligent Switching Hub

May 1995

Take Note!

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

First Edition (May 1995)

This edition applies to the 8260 Multiprotocol Intelligent Switching Hub family.

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

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 545 Building 657
P.O. Box 12195
Research Triangle Park, NC 27709-2195

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.

Abstract

This document describes the IBM 8260 Multiprotocol Intelligent Hub. It provides information about the 8260 architecture as well as how to install, configure and manage the 8260 Ethernet and token-ring media modules.

This document was written for customers, systems engineers, network professionals and technical support personnel. Some knowledge of local area networks, token-ring and Ethernet architecture is assumed.

(327 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help both IBM Customers and IBM System Engineers to install and configure the IBM 8260 Multiprotocol Intelligent Switching Hub. It contains description of the 8260 architecture as well as information about how to install, configure and manage the the 8260 Ethernet and token-ring modules. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM 8260 Multiprotocol Intelligent Switching Hub. See the PUBLICATIONS section of the IBM Programming Announcement for the 8260 for more information about what publications are considered to be product documentation.

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 program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

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 license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AIX/6000
IBM	NetView
RS/6000	

The following terms in this publication, are trademarks of other companies:

Windows is a trademark of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

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

DECnet, DEC VT100 and DEC VT220	Digital Equipment Corporation
Chipcom, ONline, ONcore	Chipcom Corporation
Novell, NetWare and IPX	Novell Corporation
Retix	Retix Corporation

Preface

This document is intended to assist customers and IBM system engineers to implement local area networks based on the IBM 8260 Multiprotocol Intelligent Switching Hub. It contains description of the 8260 architecture as well as information about how to install, configure and manage the the 8260 Ethernet and token-ring modules.

How This Document is Organized

The document is organized as follows:

- Chapter 1, “An Overview of the IBM 8260 Hub”

  This chapter is an introduction to the IBM 8260 Multiprotocol Intelligent Switching Hub.

- Chapter 2, “Backplane Architecture”

  This chapter provides details of the 8260 backplane architecture.

- Chapter 3, “8260 Fault Tolerant Controller Module”

  This chapter provides information about the 8260 fault-tolerant controller module.

- Chapter 4, “8260 Distributed Management Architecture”

  This chapter describes the 8260 Distributed Management architecture.

- Chapter 5, “8260 Intelligent Power Management Subsystem”

  This chapter describes the 8260 Intelligent Power Management Subsystem.

- Chapter 6, “8260 Intelligent Cooling Subsystem”

  This chapter describes the 8260 Intelligent Cooling Subsystem.

- Chapter 7, “8260 Ethernet Modules”

  This chapter provides detailed description and configuration information about the 8260 Ethernet modules.

- Chapter 8, “8260 Token-Ring Support”

  This chapter provides a description of the advanced features supported by the 8260 token-ring modules.

- Chapter 9, “8260 Token-Ring Modules”

  This chapter provides detailed description and configuration information about the 8260 token-ring modules.

- Chapter 10, “8260 RMON Support”

  This chapter provides an introduction to RMON as well as the RMON support by E-MAC and T-MAC daughter cards.

- Chapter 11, “8260 Multiprotocol Interconnect Module”

  This chapter provides details of routing and bridging support provided by the 8260 Multiprotocol Interconnect module.

- Appendix A, “Power Requirements for 8250/8260 Modules”

This appendix provides information about the power requirements of the 8250 modules.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

- *IBM 8260/8250 PSPG*,GA33-0285
- *IBM 8260 Installation Guide*, SA33-0251
- *8260 TR Active Media Module Port Switching Guide*, SA33-0256
- *8260 Network Interconnect Module*, SA33-0258
- *IBM 8260 (DMM) User's Guide*, SA33-0259
- *IBM 8260 Ethernet 24-Port 10BASE-T User's Guide*, SA33-0260
- *IBM 8260 Ethernet Per Port User's Guide*, SA33-0261
- *IBM 8260 Ethernet Security Module User's Guide*, SA33-0262
- *8260 DMM Commands Guide*, SA33-0275
- *IBM 8260 DMM Quick Reference Commands*, SA33-0276
- *Passive Media Module User's Guide*, SA33-0286
- *8260 Network Interconnect Module Reference Guide*, SA33-0288
- *8260 A4-FB100 Installation and User's Guide*, SA33-0324
- *IBM 8260 A-CP Switch Installation and User's Guide*, SA33-0326

International Technical Support Organization Publications

- *IBM 8250 Intelligent Hub and IBM Hub Management Program/6000*, GG24-4033

A complete list of International Technical Support Organization publications, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

To get listings of ITSO technical bulletins (redbooks) online, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

How to Order ITSO Technical Bulletins (Redbooks)

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-284-4721. Visa and Master Cards are accepted. Outside the USA, customers should contact their IBM branch office.

Customers may order hardcopy redbooks individually or in customized sets, called GBOFs, which relate to specific functions of interest. IBM employees and customers may also order redbooks in online format on CD-ROM collections, which contain the redbooks for multiple products.

Acknowledgments

The advisor for this project was:

Mohammad Shabani
International Technical Support Organization, Raleigh Center

The authors of this document are:

Mohammad Shabani
International Technical Support Organization, Raleigh Center

Nongyao Buranarachada
IBM Thailand

Mike Welsh
IBM Australia

This publication is the result of a residency conducted at the International Technical Support Organization, Raleigh Center.

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Shawn Walsh
International Technical Support Organization, Raleigh Center

Haissam Alaiwan
8260 Product Planner, La Gaude

Theodore A. Makranczy
IBM Education and Training, USA

James J. Haefele
IBM Education and Training, USA

Benton R. Hobgood
IBM 8260 Development, RTP

Bradley S. Trubey
IBM 8260 Development, RTP

Victoria S. Thio
IBM 8260 Development, RTP

Walter G. Habermas
US National Technical Support, RTP

Chapter 1. An Overview of the IBM 8260 Hub

This chapter is an introduction to the IBM 8260 Multiprotocol Intelligent Switching Hub. It is intended to provide the reader with an overview of the following:

- Hardware description
- Backplane architecture
- Fault-tolerant power subsystem
- Intelligent cooling subsystem
- Distributed management architecture
- Hot pluggability
- Fault-tolerant controller module
- Compatibility with the 8250 family

1.1 Introduction

The 8260 is an intelligent managed hub which provides the platform to build local area networks using various types of cabling systems (such as STP, UTP, fiber and coax) and different types of LAN protocols (such as token-ring, Ethernet, and FDDI). Additionally, the 8260 provides platform for the implementation of high-speed networks based on Asynchronous Transfer Mode (ATM) technology.

The 8260 is a rack-mountable hub and depending on the model it allows you to install up to 17 payload *modules*. These modules can be a combination of media and management modules providing you with the flexibility to design networks addressing the individual needs of your organization.

Media and management modules can be installed or removed from the 8260, while the hub is operational. This allows you to modify the configuration of the network with minimal disruption to the users.

The 8260 provides the room to install up to two controller modules. The second controller module will be used to provide backup for the primary controller module.

In addition to a wide range of 8260 media and management modules which are specifically designed to take advantage of the features offered by the new chassis, the 8260 supports all of the media and management modules from the 8250 (but not its controller module). This provides you with the ability to protect your investment in the 8250 modules.

Note: As the 8260 is taller than the 8250, an optional adapter kit is required to install the 8250 modules in an 8260.

The 8260 is designed to be a stand-alone unit or to be mounted in a standard 19″ rack. The 8260 is shipped with a rack mounting kit, a rubber feet kit and a cable tray assembly.

When you order the 8260, the following components will be included in the 8260 chassis which is shipped to you:

- One controller module

- One power supply
- One power supply bay cover
- One AC power cord
- Three fan units
- One cable tray
- One rack mount kit
- One rubber feet kit
- Six blank dual-slot filler plates
- Three blank single-slot filler plates

Additionally, you can order the following features to be included in your 8260:

- Up to three additional power supplies for 8260 Model 017 and Model 17 A or up to two additional power supplies for the 8260 Model 010.
- 8250 adapter kit
  - Distributed Management Module (DMM)
  - Ethernet Carrier Distributed Management Module (EC-DMM)
  - Ethernet Media Access Control (E-MAC) daughter card
  - Token-ring Media Access Control (T-MAC) daughter card
- Ethernet Modules:
  - 8260 Ethernet 24-port 10Base-T module
  - 8260 Ethernet 20-port 10Base-T module
  - 8260 Ethernet 40-port 10Base-T module
  - 8260 Ethernet 10-port 10Base-FB module
  - 8260 Multiprotocol Interconnect module
  - 8260 Ethernet Security daughter card
- Token-ring modules:
  - 18 port active per-port switching module
  - 18 port active module-switching module
  - 20 port passive module-switching module
  - Dual fiber repeater module
  - Jitter Attenuator daughter card
- ATM modules:
  - ATM Control Point and Switch module
  - 4-port ATM Concentrator module

    Note: This book will not discuss the ATM components of the 8260.

The 8260 can be managed out-of-band using an ASCII console attached locally or via modem to the management module. Additionally, you may manage the 8260 via SNMP using the Hub Manager Program for AIX.

The following sections provide an overview of the various components of the 8260.

1.2 8260 Hardware Description

There are three models of the 8260:

- 8260-017
- 8260-010
- 8260-17A

1.2.1 IBM 8260 Model 017

The 8260 Model 017 is a 17-slot module which allows you to install any combination of 8260 and 8250 modules (except the 8250 Controller module) to set up token-ring, Ethernet and/or FDDI networks. Additionally, it can be upgraded with the ATM backplane to allow you to set up an ATM network.

The 8260 Model 017 chassis is made up of 5 main areas:

- The backplane
- The payload area
- The Controller module slots
- The intelligent power subsystem
- The intelligent cooling subsystem

Figure 1 on page 4 provides a view of an 8260 multiprotocol intelligent switching hub with both 8250 and 8260 modules installed.

1.2.1.1 8260 Backplane

The 8260 Model 017 has two standard backplane buses which are used to provide you with the ability to configure token-ring, Ethernet, and/or FDDI network segments. These two backplane buses are:

- Enhanced TriChannel - Allows you to configure the following:
  - Three Ethernet segments or
  - Up to 7 token-ring segments or
  - Up to 4 FDDI segments

  You may also have a mixture of segments using different protocols. In that case, the maximum number of permitted segments will depend on the configuration of your hub.
- ShuntBus - Allows you to configure the following:
  - Two Ethernet segments and
  - 10 token-ring segments (or 4 FDDI segments)

The Enhanced TriChannel and the ShuntBus are fully described in Chapter 2, “Backplane Architecture” on page 13.

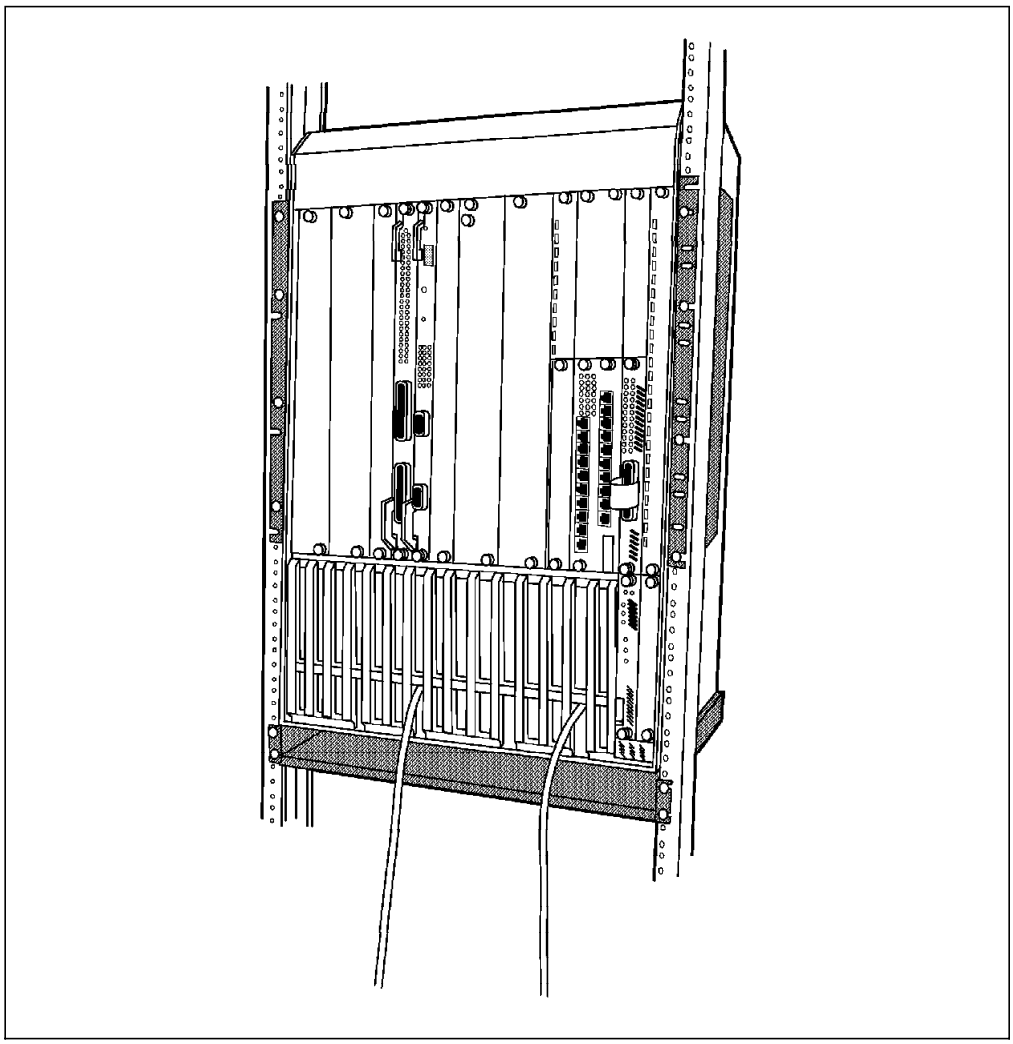


Figure 1. IBM 8260 Model 017

1.2.1.2 Payload Area

The payload area provides the housing for 17 media and management modules. In addition to the 8260 module, you may install all the 8250 modules (except the Controller module) in an 8260. Once these modules are installed on the 8260, they will be connected to the backplane.

Certain modules provide you with *per-port switching* capability, which allows you to connect different ports on the same module to different backplane segments. Other modules are *module-switching* modules, which means that all the ports on the module must be connected to the same network segment. The per-port switching capability is available for both Ethernet and token-ring.

Since the 8260 modules are taller than the 8250 modules, when you install one or more 8250 modules in the 8260 multiprotocol intelligent switching hub, you must use the *8250 Adapter Kit*. Depending on the kit that you order, the 8250 adapter kit enables you to install up to 4, 9 or 16 single-slot 8250 modules or a mixture of single-slot and dual-slot 8250 modules.

The 8250 adapter kit consists of the following:

- Right Boundary Adapter: This adapter is a full length adapter and occupies one slot. Installation of this adapter results in 16 slots remaining available in the 8260 for the installation of media and management modules. It is recommended that you install this adapter in slot 17. The reason for this is that if an 8250 management module becomes the master management module, it will always see the Controller module installed in slot 17. Therefore, if there is any other module installed in this position, it will not be recognized by the xMM.

  Note: If a DMM is the master management module, it will always be able to recognize the module installed in slot 17.

- Left Boundary Adapter: This adapter will be installed on the left boundary of the area occupied by the 8250 modules. The top portion of this adapter provides a filler plate, while the bottom-portion will provide you with the room to install an 8250 module.
- Dual-slot Top Filler: This adapter provides the filler plate for two slots of the 8260 providing you with the room to install two single-slot (or one dual-slot) 8250 module.
- Single-slot Top Filler: This adapter provides the filler plate for one slot of the 8260 providing you with the room to install a single-slot 8250 module. Note that two of these adapters can be used to install a dual-slot 8250 module.

The components of the 8250 adapter kit are shown in Figure 2.

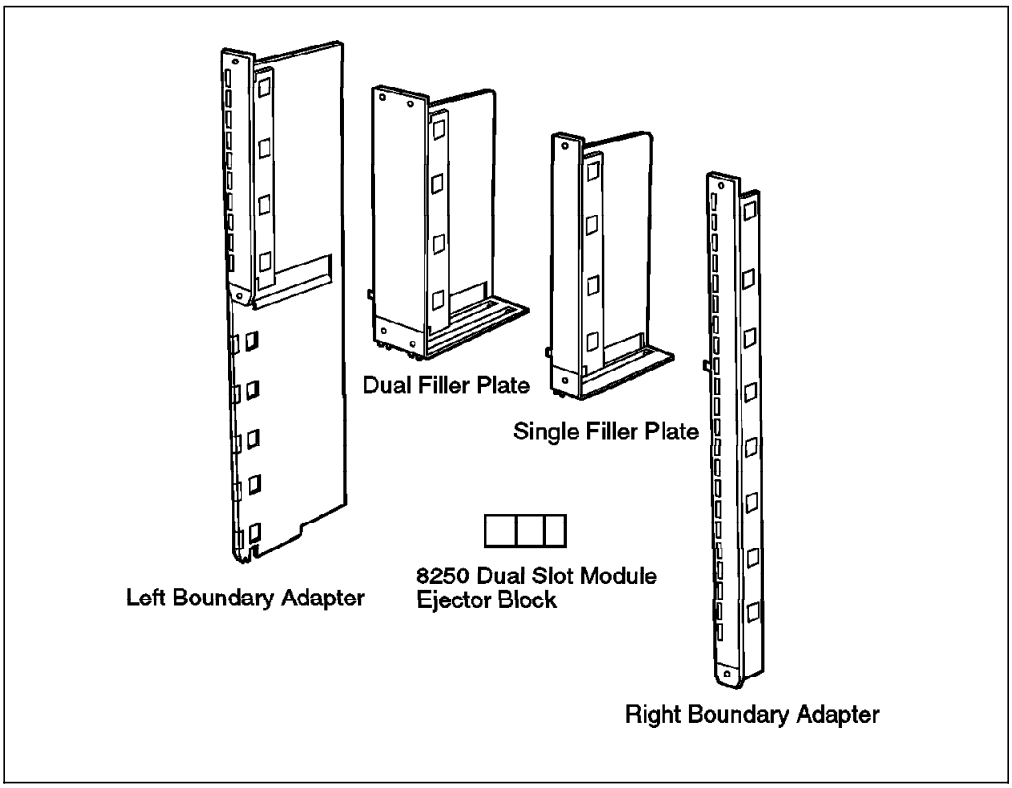


Figure 2. Components of the 8250 Adapter Kit

Table 1 on page 6 shows the quantity of each component for the various 8250 adapter kits:

Table 1. Components of the 8250 Adapter Kit for 8260			
Adapter kit Component	**4-slot Feature**	**9-slot Feature**	**16-slot Feature**
Left Boundary Adapter	1	1	1
Right Boundary Adapter	1	1	1
Dual-Slot Top Filler	1	3	7
Single-Slot Top Filler	1	2	1
Dual-Slot Module Ejector Blocks	4	9	16
8250 Module Blank Faceplate	3	8	15

1.2.1.3 Fault-Tolerant Controller Module Slots

The Controller module provides all the clocking signals for the 8260. It is also used to provide management of the power subsystem and the cooling subsystem.

The 8260 chassis has two dedicated slots for the use of the Fault-Tolerant Controller modules. These are referred to as slots 18 and 19. The 8260 Model 17 arrives with 1 Controller module as standard which is required for the operation of the 8260. You may install a second Controller module which will be used to back up the primary Controller module in case of failure. Fault tolerance is established when there are two Controller modules installed. Either module may be the master but in the event of the master Controller module failing and the standby Controller module taking over, the network *will* be disrupted.

1.2.1.4 The Intelligent Power Subsystem

The power subsystem provides an easy access power bay which can support up to four load-sharing, high capacity, managed power supplies. The 8260 Model 017 arrives with one power supply as standard and you may optionally install three additional power supplies. Features of the power subsystem are:

- Accessibility

  The power bay is easily accessed from the front of the 8260.

- Hot pluggability

  You may install or remove power supplies while the hub is operating from the other installed power supplies.

- High capacity power supplies

  Each power supply provides up to 295 watts of power.

- Load sharing capability

  The power consumption is evenly distributed over all the power supplies.

- Power management

  Using a combination of the DMM and the Controller module the power subsystem can be monitored and controlled in either fault tolerant or non-fault tolerant mode.

All of these features add up to a true seamless redundancy of the power subsystem. The intelligent power subsystem is fully described in Chapter 5, “8260 Intelligent Power Management Subsystem” on page 73.

1.2.2 The Intelligent Cooling Subsystem

The cooling subsystem consists of 3 fans, each of which cools a specific area of the hub. Each of the fans has a sensor to detect a slow or stopped condition and a temperature sensor to detect an over temperature condition. In conjunction with the Controller module and the DMM the hub environment can be monitored and controlled for over temperature conditions. Fan and Temp LEDs on the Controller module can also alert the user to potential problems. The intelligent cooling subsystem is described in detail in Chapter 6, “8260 Intelligent Cooling Subsystem” on page 91.

1.2.2.1 Distributed Management Architecture

To fully manage the 8260 and the installed modules, the 8260 uses a distributed management architecture. In this architecture, the various tasks of managing the various elements of the hub are distributed across the following elements:

- Distributed management module
- MAC daughter cards
- Controller module

There are 2 types of distributed management module (DMM):

- Stand-alone DMM
- EC-DMM

In terms of management functions, DMM and EC-DMM are identical. The only difference between these two cards is their ability to house Ethernet MAC daughter cards.

The DMM, along with the fault-tolerant Controller module, manages and controls the 8260 hub and its modules. However, to perform certain management functions such as network traffic monitoring, there is a need for a daughter card to assist DMM. There are two types of daughter cards:

- Ethernet Media Access (E-MAC) daughter card
- Token-ring Media Access (T-MAC) daughter card

The combination of DMM and daughter cards provides a cost efficient management architecture that consolidates media management into a single card, while distributing network monitoring across a series of protocol dependent daughter cards. Detailed information about the distributed management architecture of the 8260 and the management modules and daughter cards is provided in Chapter 4, “8260 Distributed Management Architecture” on page 35.

1.2.3 8260 Model 010

The 8260 Model 010 is a 10-slot intelligent hub that shares many of the advanced features of the 8260 Model 017. It differs from the Model 017 in the following areas:

- It offers 10 payload slots, rather than 17.
- It allows up to three power supplies, rather than four. The basic 8260 Model 010 is shipped with a single power supply, and up to two additional power supplies can be added later. The same power supplies are used on both models.

- Model 010 is shorter than the Model 017 (498 mm versus 673 mm), but has the same depth and width.
- Power supplies in the Model 010 are housed on the left side of the chassis whereas in the Model 017 they are housed in the bottom section.

The 8260 Model 010 shares with the Model 017 all of the following benefits:

- Supports three fan units.
- Supports two Controller module slots for redundancy. The basic model is shipped with one Controller module, and a second Controller module can be added for redundancy.
- It uses the same chassis accessories and chassis features:
  - Rack mount kit
  - Cable management tray
  - Power supplies
  - Fan units
  - Controller module
- Like the 8260 Model 017, the 8260 Model 010 is field upgradeable to support ATM.

By sharing same chassis elements, networks can be built using a mixture of Model 017s and Model 010s without an overhead for managing accessories and spare parts.

Note

In the remainder of this book, the various components of the IBM 8260 are explained assuming an 8260 Model 017.

1.3 8260 Modules and Daughter Cards

This section will give an overview of currently available 8260 modules and daughter cards and a brief description of them. Details of individual modules, the necessary steps required to configure them, and some testing scenarios will be described in the following chapters. Currently, the available 8260 modules and daughter cards can be classified as follows:

1.3.1 Ethernet Modules

1.3.1.1 8260 Ethernet 24-Port 10Base-T Module

The 8260 Ethernet 24-port 10Base-T module is single-slot module which provides two Telco connectors for supporting 24 Ethernet ports. This module provides per-port switching capability which enables you to connect each port to any of the eight Ethernet segments on the backplane.

1.3.1.2 8260 Ethernet 20-Port 10Base-T Module

The 8260 Ethernet 20-port 10Base-T module is single-slot module which provides 20 RJ-45 connectors for supporting 20 Ethernet ports. This module provides per-port switching capability.

1.3.1.3 8260 Ethernet 40-Port 10Base-T Module

The 8260 Ethernet 40-port 10Base-T module is two-slot module which provides 40 RJ-45 connectors for supporting 40 Ethernet ports. This module provides per-port switching capability.

1.3.1.4 8260 Ethernet 10-Base-FB Module

The 8260 Ethernet 10-Base-FB module is a single-slot module that provides 10 fiber ports which can be used to provide fiber backbone for Ethernet segments using IEEE 10Base-F standard. You can also use these ports for connecting to Ethernet ports using optical fiber cables. This module provides per-port switching capability and can be ordered with one of the following connector types:

- ST
- FC
- SMA

1.3.1.5 8260 Multiprotocol Interconnect Module

The 8260 Multiprotocol Interconnect module is a one or two-slot module which allows you to interconnect Ethernet, 802.3 and token-ring networks using bridging and/or routing functions. Both models provide up to 6 logical ports for attachment to Ethernet segments on the backplane, and the two-slot module provides the capability to install two I/O cards which allow you to connect it to external token-ring and Ethernet networks.

1.3.1.6 Ethernet Security Card

This is a daughter card that can be installed on any 8260 Ethernet media module and provides you with the ability to perform intrusion protection and/or eavesdropping protection for an Ethernet segment.

1.3.2 Token-Ring Modules

1.3.2.1 8260 TR 18 Port Active PPS Switch Module

The 8260 TR 18 Port Active PPS (Per-Port Switching) module is a single-slot module which provides you with 18 RJ-45 connectors for attaching up to 18 workstations to the token-ring segments on the ShuntBus using both STP and UTP cables. Using the per-port switching capability, any of the ports on this module can be connected to any of the 10 token-ring segments on the ShuntBus or 11 isolated segments on the module.

This module provides active re-timing and regeneration of the signal on every port allowing you to have longer lobe distances for both STP and UTP cabling.

Ports 17 and 18 on this module can optionally be configured to act as fully repeated RI/RO trunk ports.

1.3.2.2 8260 TR 18 Port Active Module Switching Module

The 8260 TR 18 Port Active Module Switching module is a single-slot module which provides attachment of up to 18 workstations to one of the 10 token-ring segments on the ShuntBus using both STP and UTP cables. This module provides active re-timing and regeneration of the signal on every port.

Ports 17 and 18 on this module can optionally be configured to act as fully repeated RI/RO trunk ports.

1.3.2.3 8260 TR Dual Fiber Repeater Module

The 8260 TR Dual Fiber Repeater module is a single-slot module providing 10 lobe ports with RJ-45 connectors and two RI/RO trunk ports with ST fiber connectors. Using the per-port switching feature, any of the lobes or any set of RI/RO trunk ports can be connected to any of the 10 token-ring segments on the ShuntBus.

Lobe ports support both UTP and STP cabling and each port provides active re-timing and regeneration of the signal.

The fiber RI/RO trunk ports are fully repeated and can be used for connecting your 8260 to other hubs over a distance of 2 km.

1.3.2.4 8260 TR 20 Port Passive Module-Switching Module

The 8260 TR 20 Port Passive Module-Switching module is a single-slot module which allows you to attach up to 20 workstations, which can be switched on a per module basis, to any of the 10 token ring networks on the backplane. This module allows you to use either UTP or STP cabling. Unlike the active module, it does not provide simultaneous support for both UTP and STP cabling.

1.3.2.5 8260 Jitter Attenuator Daughter Card

The 8260 Jitter Attenuator daughter card allows you to filter excessive amounts of jitter that may have accumulated in other equipment, before passing the signal to the 8260 backplane. The Jitter Attenuator daughter card can be mounted on any 8260 token-ring media module.

1.3.3 Management and Controller Modules

1.3.3.1 8260 Distributed Management Module (DMM)

The Distributed Management Module is an independent management module which allows you to fully manage and control the 8260 Multiprotocol Intelligent Hub and all the 8250/8260 modules. The DMM provides you with flexibility in handling the management of network segments with different protocols and media modules via a single management module using a single slot in the 8260 payload area. There are two different versions of DMM:

- **A Distributed Management Module with Ethernet Carrier - (DMM with Ethernet Carrier)** - The DMM with Ethernet Carrier module is a management module which is capable of housing up to 6 Ethernet MAC daughter cards.
- **A Stand-alone Distributed Management Module (Stand-alone DMM)** - the stand-alone DDM module is a management module which is not capable of housing any Ethernet MAC daughter cards.

1.3.3.2 8260 Fault-Tolerant Controller module

The 8260 Fault-Tolerant Controller Module synchronizes the operations of all installed media and management modules by providing clocking and timing to the 8260 Multiprotocol Intelligent Hub Backplane. The Controller module is also responsible for managing the power and cooling subsystems.

1.3.3.3 Ethernet Media Access Daughter Card (E-MAC)

The E-MAC daughter card allows you to gather statistics for the network to which it is attached. It can be physically mounted to either an 8260 Ethernet media module or the 8260 EC-DMM.

1.3.3.4 8260 Token-Ring Media Access Daughter Card (T-MAC)

The T-MAC daughter card allows you to gather statistics for the network to which it is assigned. It can be mounted on any 8260 token-ring media module.

Chapter 2. Backplane Architecture

The 8260 backplane consists of the following two buses:

- Enhanced TriChannel
- ShuntBus

These two buses are standard features of all the 8260 models and are installed on every 8260 shipped to the customers.

The following sections provide detailed information about the 8260 backplane and how the backplane buses operate.

2.1 LAN Segments on the Backplane

On each backplane bus (both Enhanced TriChannel and ShuntBus) there are 96 *pins* which are used for passing the network traffic between the media modules installed in the hub as well as the control signals between the media modules, fault-tolerant Controller module, and Distributed Management Module (DMM). The control signals are used to carry clocking, voltage, status and other information pertinent to the proper operation of the hub and the installed modules.

On the Enhanced TriChannel, 54 pins are available to be used for passing network traffic. the rest of the pins are used for non-data traffic signals. These signals are used for passing control signals between the Controller module and the media modules as well as signals between the Management module and the media modules. More information about these non-data traffic signals are provided in 2.5.1, “Management Buses” on page 26.

On the Enhanced TriChannel, the pins used for passing the network traffic are not permanently allocated to a specific type of network. Instead a pin may be configured to be used for passing either token-ring, Ethernet or FDDI packets at any one time. This enables more efficient utilization of the backplane resources.

The following is the maximum number of permitted LAN segments when a single protocol is used on the Enhanced TriChannel:

- 6 Ethernet segments or
- 7 token-ring segments or
- 4 FDDI segments

Note that you are allowed to have a mixture of token-ring, Ethernet and FDDI segments on the Enhanced TriChannel. In this case, the exact number of each network type which is allowed in a mixed protocol environment depends on the configuration of your hub. For detailed information about the permitted configurations in a mixed protocol environment please refer to 2.5, “Network Allocations on the 8260 Backplane” on page 23.

Figure 3 on page 14 provides an overview of the Enhanced TriChannel bus.

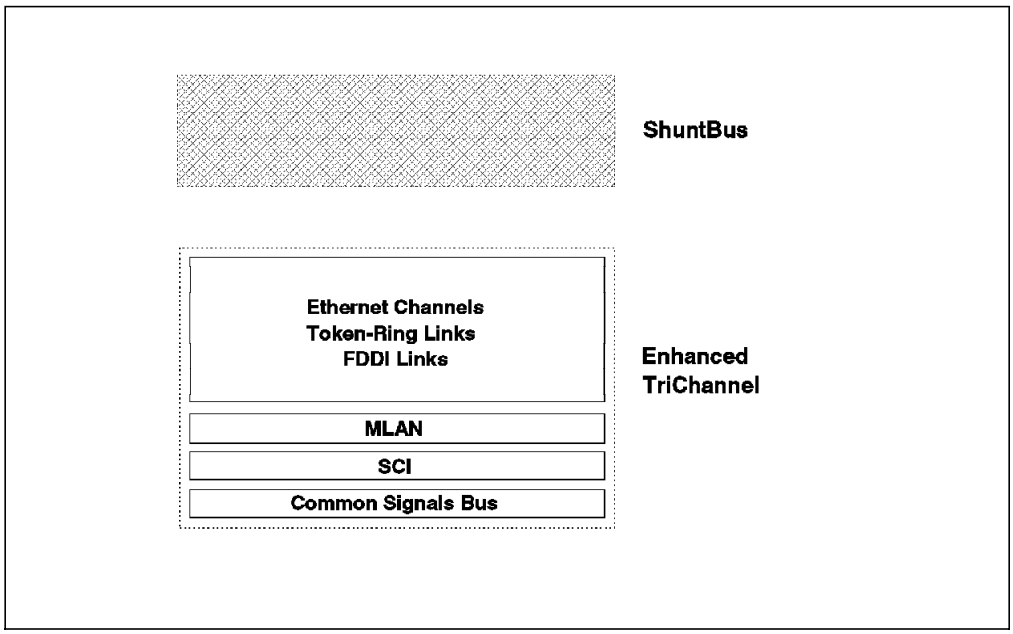


Figure 3. Enhanced TriChannel Bus

The number of pins available for user traffic on the ShuntBus is 72 pins. These pins are used to set up 2 dedicated Ethernet segments as well as 10 token-ring (or 4 FDDI) segments as shown in Figure 4 on page 15.

On the ShuntBus, 8 pins out of the 72 network traffic pins are dedicated to be used by two Ethernet segments. These dedicated pins are not available to be used by other segment types. The remaining 64 pins on the ShuntBus are available to be used by token-ring and/or FDDI segments. This allows you to have a mixture of token-ring and FDDI segments as well as two Ethernet segments on the ShuntBus. The rules governing the maximum number of FDDI and token-ring segments allowed in a mixed token-ring and FDDI environment are discussed in 2.5, “Network Allocations on the 8260 Backplane” on page 23.

The following is the permitted maximum number of LAN segments on the ShuntBus:

- 2 Ethernet and
- 10 token-ring or 4 FDDI

Note

At the time of writing this publication, there are no FDDI modules available that can be assigned to the FDDI segments on the ShuntBus. Therefore, practically, the ShuntBus allows you to have two Ethernet segments plus 10 token-ring segments.

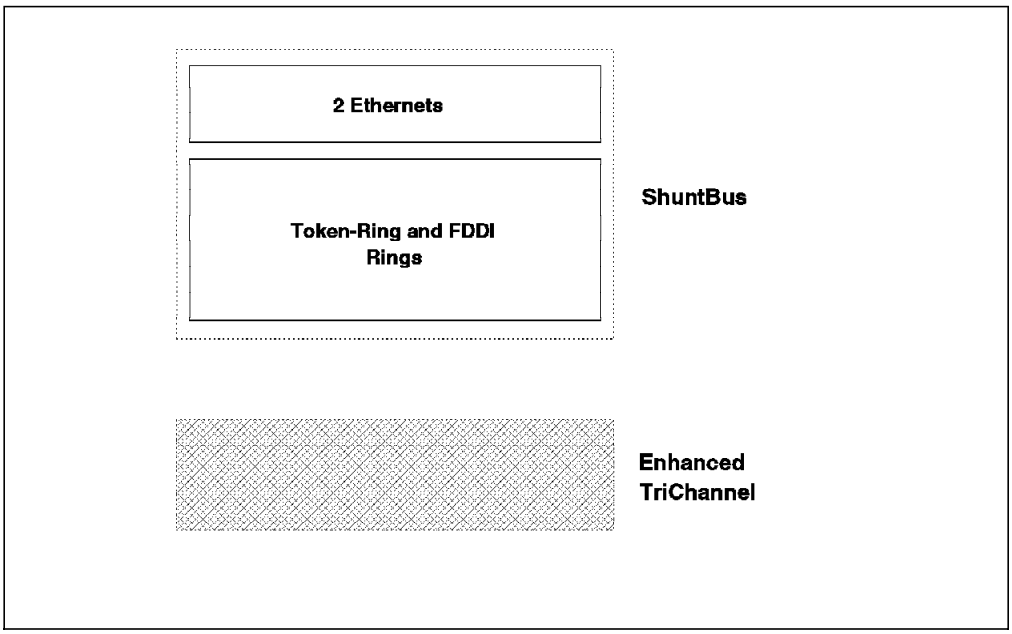


Figure 4. 8260 ShuntBus

2.2 Ethernet Segments on the Backplane

The 8260 allows you to set up a maximum of 6 Ethernet (ethernet_1 thru 6) segments on the Enhanced TriChannel and two Ethernet segments (ethernet_7 and 8) on the ShuntBus. ethernet_1 thru 3 can consist of 8250 and/or 8260 Ethernet modules, whereas ethernet_4 thru 8 can consist of 8260 Ethernet modules only.

Each Ethernet segment on the backplane uses a number of pins on the backplane which is referred to as an *Ethernet Path* in this document. There are 8 Ethernet paths (ethernet_path_1 thru 8) on and 8260. ethernet_path_1 thru 6 are on the Enhanced TriChannel whereas ethernet_path_7 and 8 are on the ShuntBus.

Ethernet_path_1 thru 3 use 14 pins each to set up an Ethernet segment while ethernet_path_4 thru 8 use 4 pins each.

The Ethernet segments on the Enhanced TriChannel use the same pins on the backplane as are used by the token-ring and/or FDDI segments. Therefore, simultaneous configuration of other types of networks (such as FDDI and/or token-ring) on your hub′s Enhanced TriChannel will impact the number of Ethernet networks available for use. However, the two Ethernet segments on the ShuntBus have dedicated pins on the backplane and will not be impacted by the configuration of other segment types (that is, token-ring and/or FDDI) on the ShuntBus.

Each Ethernet segment on the 8260 utilizes one of the Ethernet paths on the backplane regardless of the number of Ethernet modules which constitute that segment. You can choose the Ethernet network (hence the Ethernet path used by your module) using the following management command:

```
SET MODULE {slot.sublsot} NETWORK {ethernet_n} or

SET PORT {slot.port} NETWORK {ethernet_n}
```

Before assigning the port or module to a network you may use the following management command to display the availability of the Ethernet segments on the Enhanced TriChannel and the ShuntBus:

```
SHOW BACKPLANE_PATHS ETHERNET
```

An example of the output from this command is shown in Figure 5.

```
8260> show backplane_paths ethernet

Physical Path            Logical Network
---------------          ---------------
ETHERNET_PATH_1          ETHERNET_1
ETHERNET_PATH_2          in use
ETHERNET_PATH_3          in use
ETHERNET_PATH_4          available
ETHERNET_PATH_5          ETHERNET_5
ETHERNET_PATH_6          ETHERNET_6
ETHERNET_PATH_7          ETHERNET_7
ETHERNET_PATH_8          ETHERNET_8

8260>
```

Figure 5. Backplane Path Display for Ethernet Segments

In this example, the Ethernet segments shown ″in use″ are not available to be used for setting up Ethernet segments in this hub due to the backplane pins corresponding to these segments being currently used by other segment types such as token-ring and/or FDDI. Ethernet_1 and ethernet_5 through ethernet_8 are currently configured to be used by Ethernet modules in this hub. The pins available to be used by ethernet_4 are not currently configured to be used by any network type.

To connect and use the Ethernet segments on the backplane (Enhanced TriChannel or ShuntBus) various techniques are used by the various 8250 and 8260 Ethernet modules. These techniques can be categorized into one of the three following methods:

- Method 1:

  This method uses 14 pins on the backplane to set up an Ethernet segment. In this method, each module attached to the Ethernet segment will send the slot-id and port-id of the transmitting station in *parallel* over the backplane. The slot-id will use 5 pins and the port-id will use 4 pins on the backplane as shown in Table 2 on page 17.

  The slot-id will be used to perform *digital collision detection* as described in 2.2.1, “Digital Collision Detection” on page 19. Additionally, the slot-id and the port-id will be used by the management module to perform statistics gathering about the segment as well as the individual ports and modules on that segment as described in 2.2.3, “Statistics Collection” on page 19.

  This method is used by all 8250 modules and is only allowed on ethernet_1, ethernet_2, and ethernet_3 segments on the Enhanced TriChannel. Therefore, the 8250 Ethernet modules installed in the 8260 can only be assigned to these three segments and can not be assigned to Ethernet

segments ethernet_4, ethernet_5 and ethernet_6 on the Enhanced TriChannel and ethernet_7 and ethernet_8 on the ShuntBus.

- Method 2:

  This method also uses 14 pins on the backplane to set up an Ethernet segment. In this method, each module attached to that Ethernet segment will use digital collision detection identical to that used in method 1. This means that the modules will send their slot-id in parallel over the backplane. However, to allow the management module to collect statistics about these modules, they send the slot-id and port-id in serial over a single pin on the backplane.

  This method is used by the 8260 modules when connected to ethernet_1, ethernet_2, and ethernet_3 segments on the Enhanced TriChannel.

  Method 2 is compatible with method 1. That is, modules using method 1 and 2 can be assigned to the same Ethernet LAN segment. Therefore, you may set up ethernet_1, thru ethernet_3 to consist of a mixture of the 8250 and/or 8260 Ethernet modules.

- Method 3:

  This method uses only four pins on the backplane to set up an Ethernet segment. In this method, each module will send its slot-id and port-id in serial over a single pin on the backplane. This information allows the management module to collect statistics about the modules and ports.

  For collision detection, the modules using this method rely on an *analog collision detection* as described in 2.2.2, “Analog Collision Detection” on page 19.

  This method is used by the 8260 modules when connected to ethernet_4, ethernet_5, and ethernet_6 segments on the Enhanced TriChannel as well as ethernet_7 and ethernet_8 segments on the ShuntBus.

  This method is not compatible with methods 1 and 2. Therefore, ethernet_4 thru ethernet_8 segments can consist of 8260 Ethernet modules only.

Table 2 gives a breakdown of the pins which are used by 8250 and 8260 Ethernet modules when using the above methods.

Table 2 (Page 1 of 2). Ethernet Pins on the 8260 Backplane

Description	**Method 1**	**Method 2**	**Method 3**	
Data enable signal	Y	Y	Y	
Data in NRZ format	Y	Y	Y	
Local collision	Y	Y	N/A	
Remote collision	Y	N	N/A	
Analog collision	N/A	N/A	Y	
Port ID bit 0 (lsb)	Y	N	N/A	
Port ID bit 1	Y	N	N/A	
Port ID bit 2	Y	N	N/A	
Port ID bit 3 (msb)	Y	N	N/A	
Slot ID bit 0 (lsb)	Y	Y	N/A	
Slot ID bit 1	Y	Y	N/A	
Slot ID bit 2	Y	Y	N/A	

Table 2 (Page 2 of 2). Ethernet Pins on the 8260 Backplane				
Description	**Method 1**	**Method 2**	**Method 3**	
Slot ID bit 3	Y	Y	N/A	
Slot ID bit 4 (msb)	Y	Y	N/A	
Serial ID	N	Y	Y	

The following is a brief description of the use of each of the pins in an Ethernet segment on the 8260 backplanes:

- *Data enable signal*:

  When this signal is active, data on the backplane is valid and the modules should receive and process the data on the ′Data in NRZ Format′ pin.

- *Data in NRZ format*:

  This signal is used to transmit data on the backplane in NRZ format.

- *Local collision*:

  This signal is used to indicate local collisions on the backplane. It is raised when two or more modules on the same segment are transmitting data at the same time. It is also raised if two or more ports on the same module transmit simultaneously.

- *Remote Collision*:

  This signal is raised when a collision occurs in a remote hub. This signal is only used by the 10Base-FB modules.

- *Port-ID:*

  Whenever an Ethernet module using method 1 transmits data on the backplane, it must sent the port-id of the transmitting port on these pins.

  The Management module will use the port-id and slot-id (see below) signals to find out which port and module is sending the data on the ′Data in NRZ Format′ pin; hence, it is able to collect and report per-port statistics.

  Note: Since four pins are used to transmit the port ID in parallel, the per-port statistics cannot be reported for all the ports of the 24-port modules. On a 24-port module, you can collect statistics about the first 12 ports only.

- *Slot ID*:

  Whenever an Ethernet module is using method 1 or 2 to transmit data on the backplane, it must send its slot-id on these five pins. This information is used for two purposes:

  1. Digital collision detection
  2. Statistics collection

- *Serial-ID*:

  This pin is used to transmit the port-id and slot-id, over the backplane, in serial format. Its purpose is to provide the Management module with a way to collect per-port and per-module statistics for modules using method 2 and 3.

- *Analog Collision*:

This pin is used to provide a means of detecting collisions of the segments using method 3. Analog collision detection is described in 2.2.2, “Analog Collision Detection” on page 19.

2.2.1 Digital Collision Detection

Collision detection on the backplane (for methods 1 and 2) is done by using slot-id information transmitted on the backplane. Each module asserts its own slot-id one bit time before transmitting user data on the data pin. The following bit time, the module reads the slot-id received on these pins and compares it with its own slot-id. If only one module is transmitting, the transmitted and received slot-id values are the same and no collision exists. If more than one module is transmitting, then at least one module will detect an unequal slot-id comparison and will then signal local collision.

It should be noted that slot-id mismatches will not always occur in all modules involved in a collision. This is because, the slot-id sent on the bus is the ′OR′ of the two or more slot-ids transmitted by the individual modules. For example, if the module in slot 8 (B′0111′) collides with the module in slot 1 (B′0000′), the backplane will ″OR″ the two together and both modules will see B′0111′. This will look all right to the module in slot 8, so it will not assert the local collision pin. However, the module in slot 1 will detect the slot-id mismatch and will assert the local collision pin.

2.2.2 Analog Collision Detection

To perform analog collision detection, a current source is used to generate a level on the backplane. Each time a module starts transmitting, the voltage on the backplane drops. If more than one module is transmitting at the same time, the drop at the voltage level is used to detect such a condition.

2.2.3 Statistics Collection

The slot-id in conjunction with the port-id and the user data is used by the Management module to collect statistical information about the ethernet_1, ethernet_2 or ethernet_3 segment as well as the individual ports and modules on that segment. For method 1 the slot-id and port-id are sent by the module in parallel over 9 pins on the backplane, whereas, modules employing methods 2 and 3 use a single pin on the backplane to transmit their slot-id and port-id.

2.3 Token-Ring Segments on the Backplane

The 8260 allows you to set up a maximum of 7 token-ring segments on the Enhanced TriChannel using the 8250 modules. Also, you can set up 10 token-ring segments on the ShuntBus using the 8260 token-ring modules. Note that the 8250 token-ring modules only connect to the Enhanced TriChannel and the 8260 modules only connect to the ShuntBus; therefore, if you want to set up a token-ring segment consisting of these two different types of modules, you must connect the segments together using RI/RO connections, bridges, or routers.

Each 8250 token-ring module which is assigned to one of the 7 token-ring networks on the Enhanced TriChannel uses one of the resources called a *token-ring path*. There are 15 token-ring paths on the Enhanced TriChannel and they are referred to as tr_path_8250_1 through tr_path_8250_15. Each token-ring path utilizes 4 pins on the Enhanced TriChannel. These pins are as follows:

- Data-in
- Clock-in
- Data-out
- Clock-out

When you assign an 8250 token-ring module to one of the token-ring networks on the Enhanced TriChannel (tr_8250_1 through tr_8250_7) using the following command:

```
SET MODULE {slot.sublsot} NETWORK {token_ring_n}
```

The 8260 will automatically allocate one of the available token-ring paths to this module. Note that you can neither choose the path used by the module, nor determine which path is used by a specific module. However, you can determine all token-ring paths on the Enhanced TriChannel which are currently being allocated in your hub by using the following management module command:

```
SHOW BACKPLANE_PATHS TOKEN_RING
```

An example of the output from this command is shown in Figure 6.

```
8260> show backplane_paths token_ring

Physical Path            Logical Network
---------------          ---------------
TR_PATH_8250_1           in use
TR_PATH_8250_2           in use
TR_PATH_8250_3           in use
TR_PATH_8250_4           in use
TR_PATH_8250_5           in use
TR_PATH_8250_6           in use
TR_PATH_8250_7           TR_8250_1
TR_PATH_8250_8           available
TR_PATH_8250_9           TR_8250_1
TR_PATH_8250_10          available
TR_PATH_8250_11          in use
TR_PATH_8250_12          in use
TR_PATH_8250_13          TR_8250_1
TR_PATH_8250_14          available
TR_PATH_8250_15          available

8260>
```

Figure 6. Token-Ring Backplane Path Display

The number of token-ring paths used by a single token-ring network on the Enhanced TriChannel equals the number of token-ring modules on that network.

Note that the token-ring paths on the Enhanced TriChannel use the same pins on the backplane as are used by the Ethernet and/or FDDI segments. Therefore, simultaneous configuration of other types of networks in your hub will impact the number of token-ring networks allowed in your hub. In Figure 6, the token-ring paths shown as in ″in use″ are those backplane pins that are used by other segment types (that is, Ethernet or FDDI), whereas tr_path_8250_7, tr_path_8250_9 and tr_path_8250_13 are used to configure a single token-ring segment (tr_8250_1) consisting of three 8250 token-ring modules. Also, note that

the token-ring paths marked as ″available″ are the parts of the Enhanced TriChannel that are not currently used by any type of network.

On the ShuntBus, in addition to the two dedicated Ethernet segments, there are 10 token-ring segments. Unlike, the Enhanced TriChannel, there is no concept of token-ring paths on the ShuntBus. Instead, there are 10 physical rings on the backplane. Each of these rings is a set of 6 pins which is routed from slot to slot on the backplane and is completed across each slot via a self-shorting connector. At the end of the backplane, the signal path is returned from slot 17 to slot 1. In this manner, a ring is formed. When a module is inserted into the backplane, the self-shorting connector opens and the signal is routed onto the module. Therefore, any installed token-ring module on the ShuntBus has access to any of the 10 token-ring segments on the backplane. This design allows the implementation of per-port switching for the token-ring modules so that individual ports on a module can be assigned to different rings on the backplane. This concept is shown in Figure 7. Details of the per-port switching feature for token-ring modules is provided in Chapter 8, “8260 Token-Ring Support” on page 129.

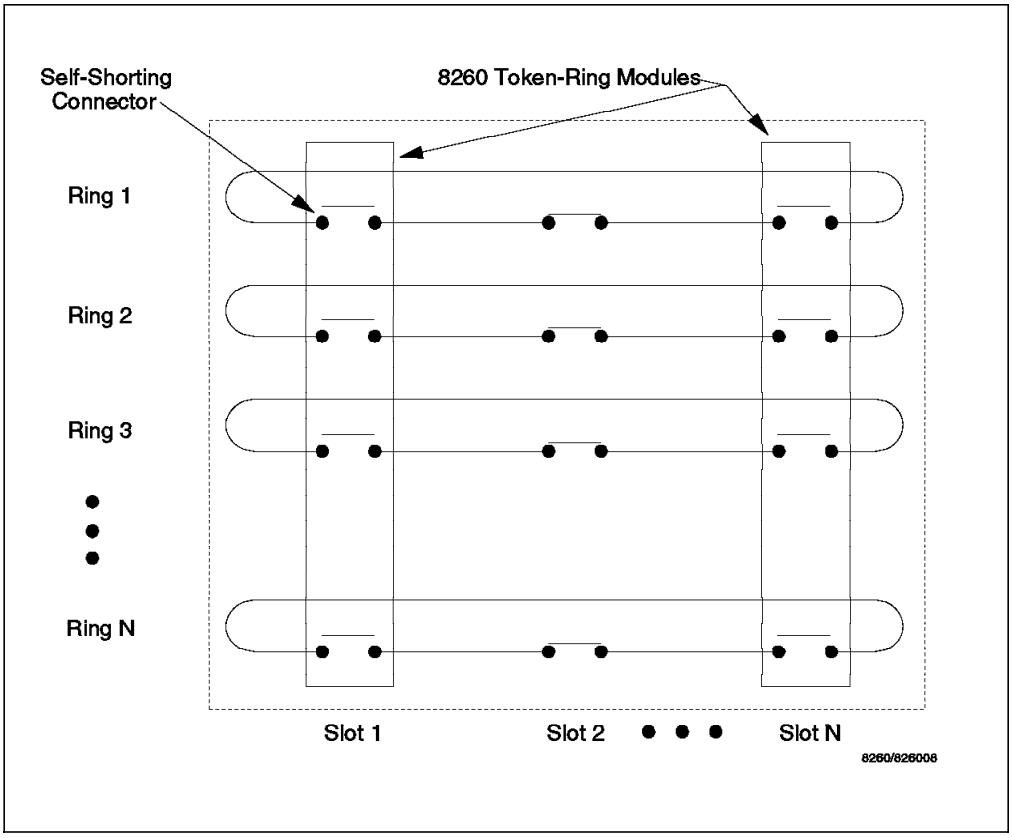


Figure 7. ShuntBus and Token-Ring

Each token-ring interface on the ShuntBus connector uses three Shunt pairs (low resistance connectors) to form one token-ring network on the backplane. The three Shunt pairs carry a clock and two data signals.

When a token-ring module is inserted into the ring, the 3 Shunt pairs connect to 6 signal lines on the module as:

- Clock transmit
- Data A transmit

- Data B transmit
- Clock receive
- Data A receive
- Data B receive

The reasons for two signals for each of the transmit and receive signals is given in 8.2, “8260 Backplane Signalling for TR Segments” on page 134.

Note that regardless of the number of token-ring modules used in a segment, you always have the ability to set up 10 separate token-ring segments on the ShuntBus.

The same pins that are used for token-ring segments on the ShuntBus are designed to be used for FDDI segments as well. Therefore, if you have a mixture of token-ring and FDDI segments on the ShuntBus, the maximum number of token-ring segments would be lower, depending on the number of FDDI segments. However, this is a theoretical limitation for the time being, as currently IBM is not offering any 8260 FDDI modules.

2.4 FDDI Segments on the Backplane

The 8260 allows you to set up a maximum of 4 FDDI segments on the Enhanced TriChannel using the 8250 modules. Also, it is possible to set up a maximum of 4 FDDI segments on the ShuntBus, using the 8260 FDDI modules. However, as there are no 8260 FDDI modules available yet, if you are planning to have FDDI segments on the 8260, you must use the 8250 FDDI modules to set up FDDI segments on the Enhanced TriChannel only.

Each FDDI module which is assigned to one of the four FDDI networks on the Enhanced TriChannel uses one of the resources called *FDDI path*. There are 8 FDDI paths on the Enhanced TriChannel and are referred to as fddi_path_8250_1 through fddi_path_8250_8. Each FDDI path utilizes 6 pins of the Enhanced TriChannel. These pins are as follows:

- Data-in
- Symbol parity-in
- Clock-in
- Data-out
- Symbol parity-put
- Clock-out

When you assign an FDDI module to one of the four FDDI networks on the Enhanced TriChannel (fddi_1 through fddi_4), using the following command:

```
SET MODULE {slot.sublsot} NETWORK {FDDI_n}
```

the 8260 will automatically allocate one of the available FDDI paths to this module. Note that you can neither choose the path used by a module, nor determine which path is used by a specific module. However, you can determine all the FDDI paths on the Enhanced TriChannel which are currently being used in your hub by using the following management module command:

```
SHOW BACKPLNE_PATHS FDDI
```

An example of the output from this command is shown in Figure 8 on page 23.

```
8260> show backplane_paths fddi

Physical Path            Logical Network
---------------          ---------------
FDDI_PATH_8250_1         in use
FDDI_PATH_8250_2         in use
FDDI_PATH_8250_3         in use
FDDI_PATH_8250_4         in use
FDDI_PATH_8250_5         in use
FDDI_PATH_8250_6         in use
FDDI_PATH_8250_7         in use
FDDI_PATH_8250_8         available

8260>
```

Figure 8. Backplane Path Display for FDDI Segments

The number of FDDI paths used by a single FDDI network on the Enhanced TriChannel equals the number of FDDI modules on that network.

The FDDI paths on the Enhanced TriChannel use the same pins on the backplane as are used by the Ethernet and/or token-ring segments. In Figure 8, the FDDI paths shown as ″in use″ are those backplane pins which are used by other segment types (that is, token-ring and/or Ethernet). Also, note that in this example, we had no FDDI modules installed in our 8260.

On the ShuntBus, in addition to the two dedicated Ethernet segments, there can be up to 4 FDDI segments. Unlike, the Enhanced TriChannel, there is no concept of FDDI paths on the ShuntBus. Instead, there are 4 FDDI networks, each using 14 pins. The FDDI segments on the ShuntBus use the same pins as the token-ring segments.

2.5 Network Allocations on the 8260 Backplane

As we now have so many options of switching modules and ports between networks it is perhaps a good time to clarify the rules regarding those allocations.

- 8250 Ethernet ports or modules can be connected to parallel addressed segments (ethernet_1 thru 3 on the Enhanced TriChannel) only.
- 8250 Ethernet ports or modules cannot be connected to serially addressed segments (ethernet_4 thru 8) on either the TriChannel or ShuntBus.
- 8260 Ethernet ports or modules can be connected to any of the segments (ethernet_1 thru 8) on the TriChannel or ShuntBus. When connected to ethernet_1 thru 3, they use parallel addressing and when connected to ethernet_4 thru 8 they use serial addressing.
- 8250 token-ring or FDDI modules can only be connected to the segments on the Enhanced TriChannel. They cannot be connected to the segments on the ShuntBus.
- 8260 token-ring (or future 8260 FDDI) modules cannot be connected to any segment on the Enhanced TriChannel. They can only be connected to the segments on the ShuntBus.

- Any module can plug into any slot and all allocation of modules to networks or channels, regardless of whether they are TriChannel or Shunt Bus, is done by electronic switching (via DIP switches on the modules or management module commands).

Figure 9 shows the Enhanced TriChannel network allocation and how the mixing of various network types affect the availability of the others.

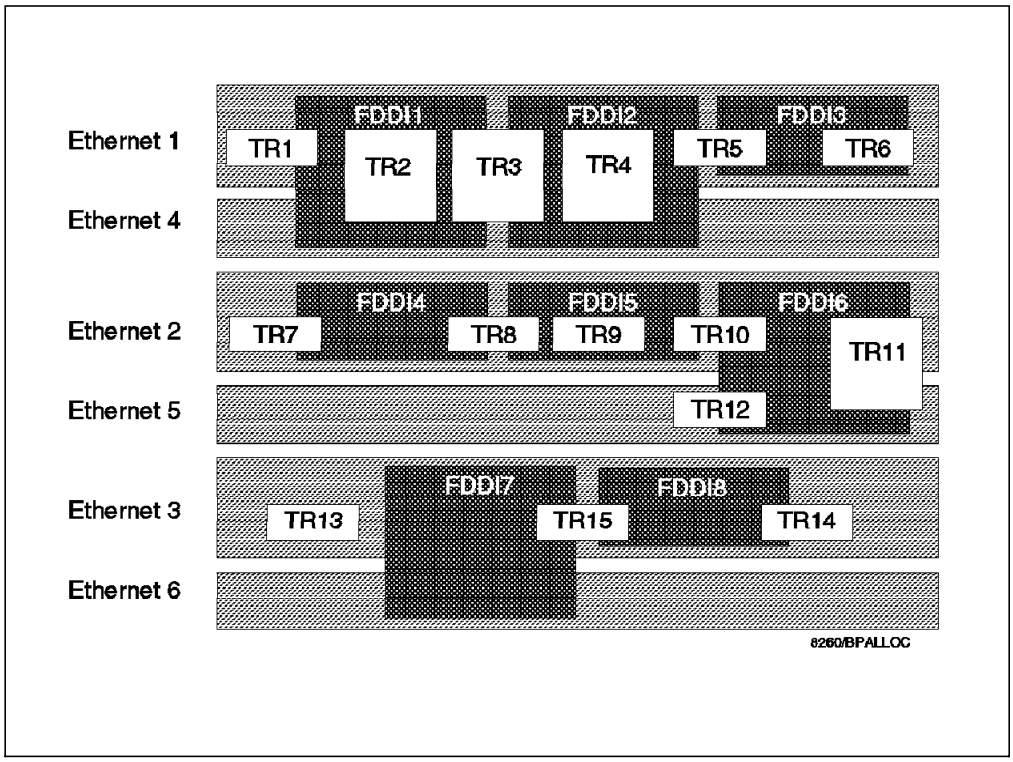


Figure 9. TriChannel Backplane Network Allocation

Using Figure 9 you can see that if, for example, tr_path_8250_3 path is used it eliminates ethernet_path_1, ethernet_path_4, fddi_path_8250_1 and fddi_path_8250_2. If ethernet_path_5 is used it eliminates tr_path_8250_11, tr_path_8250_2 and fddi_path_8250_6.

Figure 10 on page 25 illustrates the possible combinations of the network segments on the ShuntBus. In this diagram, we have shown the token-ring networks as TR 16 thru 25 and FDDI networks as FDDI9 thru 12. This is to provide a distinction between the segments on the Enhanced TriChannel and the ShuntBus for our discussion in this book. However, when you use the management module commands to assign the token-ring modules to the token-ring segments on the backplane, you will refer to the Enhanced TriChannel segments as token_ring_1 thru 7 and to the ShuntBus segments as token_ring_1 thru 10. In other words, some token-ring segments on the Enhanced TriChannel have identical names to the token-ring segments on the ShuntBus. However, the management module is programmed to realize that when you refer to a token_ring segment number when issuing a command for the 8250 module, that segment is on the Enhanced TriChannel and when the command is issued for an 8260 module, the referenced segment number is on the ShuntBus. This is, of course, due to the fact that 8250 token-ring modules can only be connected to the Enhanced TriChannel, and the 8260 token-ring modules can only be connected to the ShuntBus.

Using Figure 10 on page 25 you can see that if, for example, fddi_1 network on the ShuntBus is used, it eliminates token_ring_1, token_ring_2 and token_ring_3. Also, you can see that the use of Ethernet segments ethernet_7 and ethernet_8 have no affect on the availability of token-ring and FDDI segments.

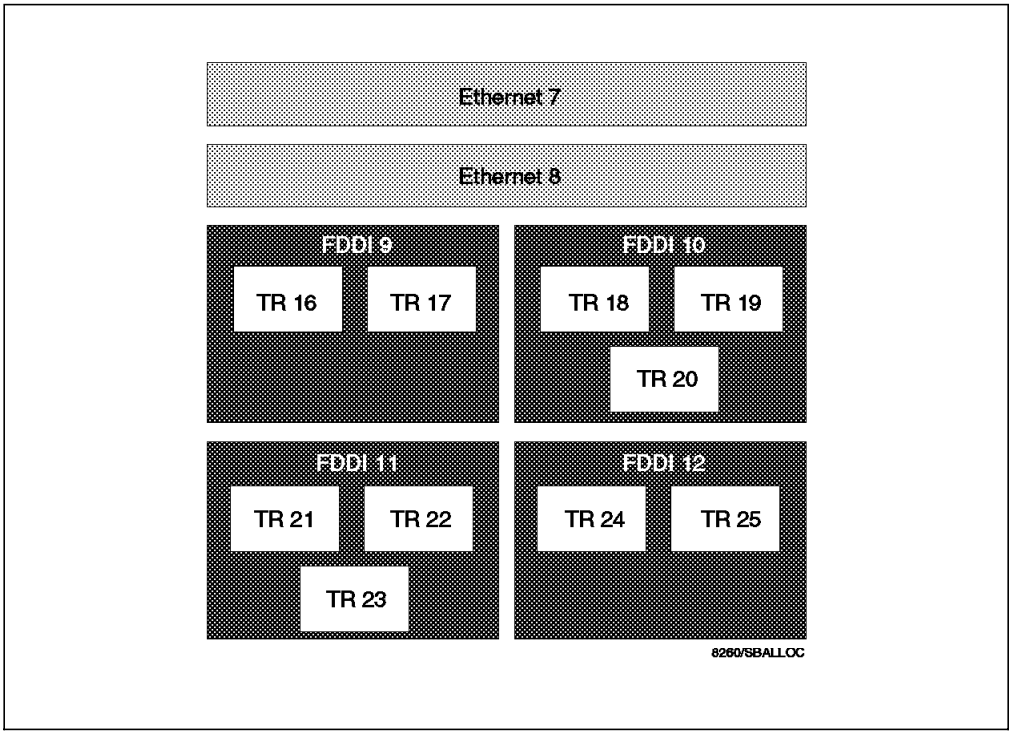


Figure 10. ShuntBus Backplane Network Allocation

Figure 11 on page 26 is a summary of how the Enhanced TriChannel and the ShuntBus are used to accommodate the various types of networks. Note that in this diagram, for the sake of avoiding a crowded picture, the token-ring and FDDI segments on the Enhanced TriChannel are not shown.

In designing your network, if possible, it is recommended that you use the Enhanced TriChannel as well as the two dedicated Ethernet segments on the ShuntBus for the Ethernet segments only and use the ShuntBus for the token-ring segments only.

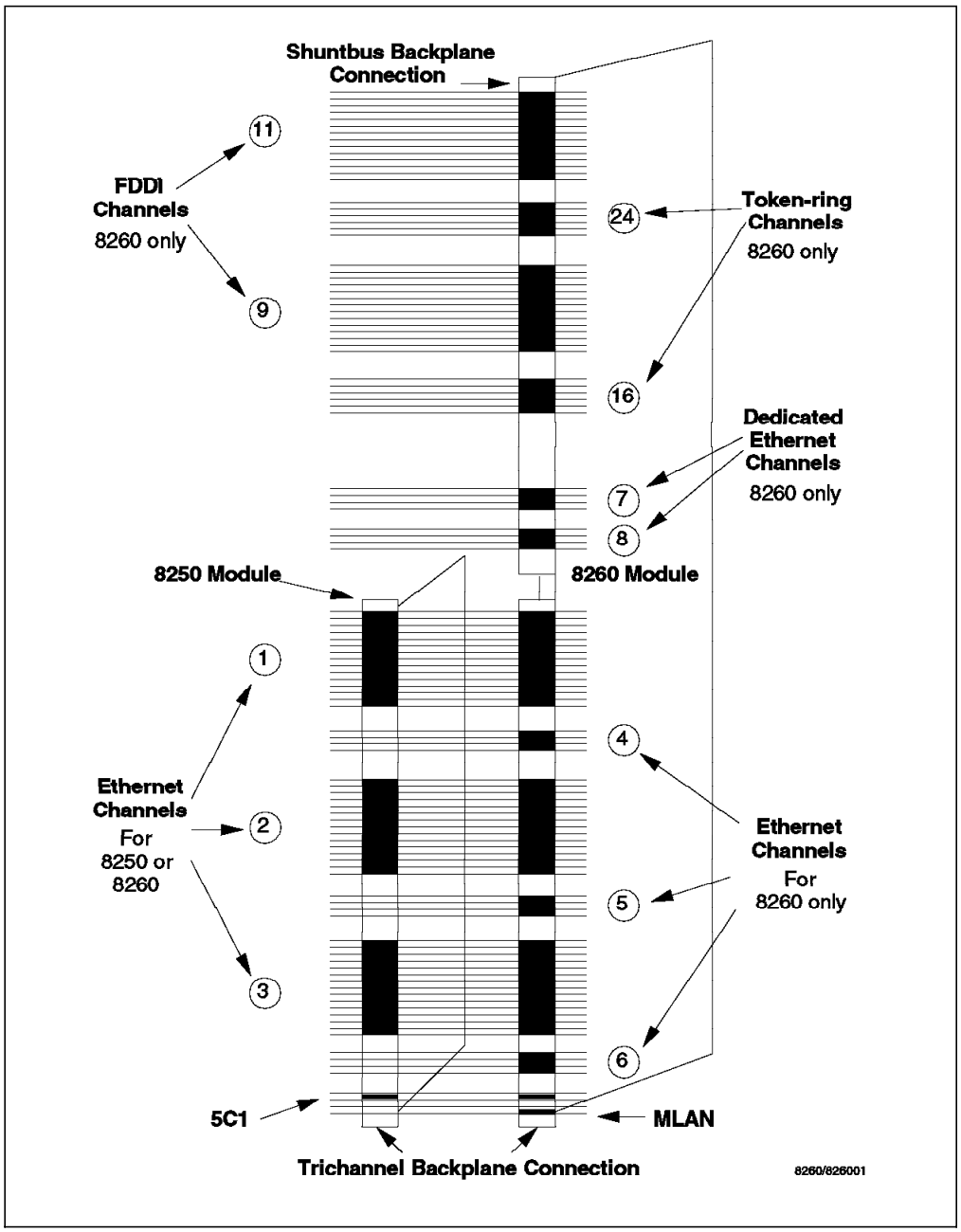


Figure 11. The Backplane Relationship between TriChannel and ShuntBus

2.5.1 Management Buses

It was mentioned earlier that 42 of the 96 pins on the TriChannel Backplane are reserved for non-data traffic. Included in these pins are the Management LAN (MLAN) and the Serial Control Interface (SCI).

2.5.1.1 The Management LAN (MLAN)

The MLAN is a dedicated 10 Mbps Ethernet bus which connects the DMM (Distributed Management Module) and all the Media Access Control daughter cards (E-MAC or T-MAC). The MAC daughter cards connect to their respective networks, T-MAC to token-ring and E-MAC to Ethernet, and provide statistics about those networks to the DMM via the MLAN. Also, the IP stack provided by

the MAC daughter card is accessed by the upper layer protocol stacks within the DMM (SNMP, Telnet) through the MLAN.

The E-MAC can be installed on either the EC-DMM or the 8260 media modules. When installed on the 8260 media modules, E-MAC can collect statistics about all the Ethernet segments on the backplane, but will not be able to collect per-port or per-module statistics for the 8250 modules which are on Ethernet_1, 2 and 3. This is due to the fact that the 8250 modules will be using parallel addressing on the backplane while the EMAC installed on the 8260 media modules will only be able to collect statistics from the serial pins. However, if the E-MAC is installed on the EC-DMM, it will be able to collect a full range of statistical information about any segment that it is attached to, regardless of whether that segment is using parallel or serial addressing. This is because the EC-DMM provides parallel to serial address translation.

Also note that E-MAC is always able to collect full statistics about 8260 modules irrespective of which type of module (EC-DMM or 8260 media modules) the E-MAC is installed on and which networks the 8260 modules are attached to.

2.5.1.2 The Serial Control Interface (SCI)

The SCI is the same as that used in the 8250. All modules, 8250 and 8260 alike, use the SCI to transmit module and port configuration data. The controller module uses the SCI to gather VPD from the modules, and to get power and cooling status. The controller module, in conjunction with the DMM, also uses the SCI as a medium to change the status of power supply to the modules and to remove and add modules in the event of a change in the power or cooling subsystems. Figure 12 illustrates the relationship between the MLAN, SCI and the modules.

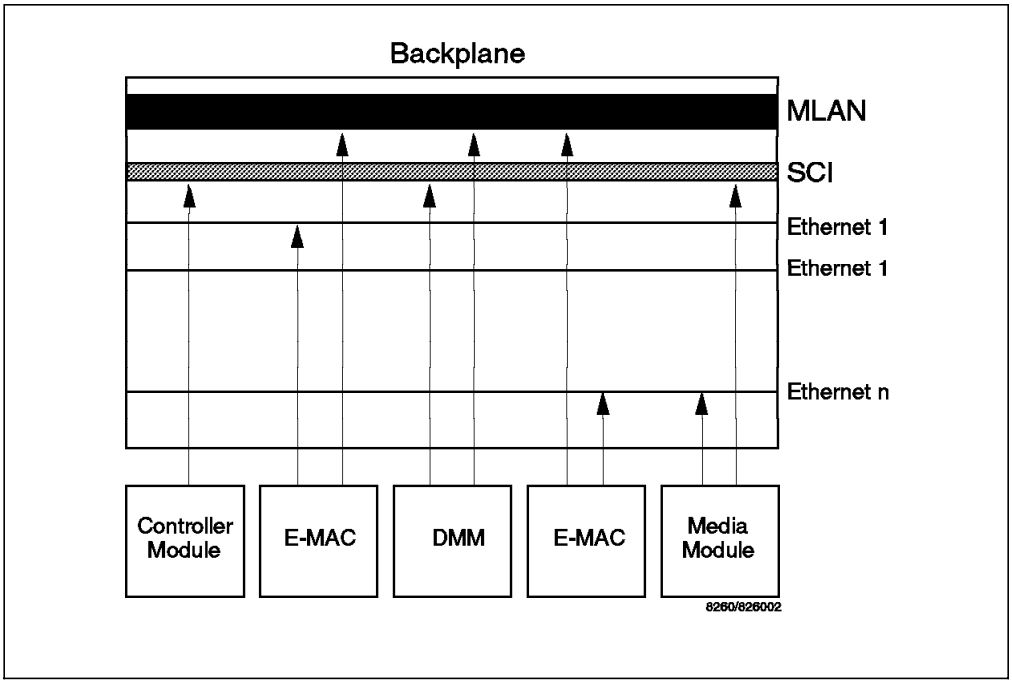


Figure 12. 8260 Management Buses

Chapter 3. 8260 Fault Tolerant Controller Module

The 8260 Fault Tolerant controller module is a critical component of the 8260. One active controller module is always required in order to keep the 8260 hub operational and running. Unlike the 8250 controller module, the 8260 Fault Tolerant Controller module does not occupy any of the payload slots because it resides on either slot 18 and/or 19 in the hub which are reserved for the controller modules. This chapter provides you with detailed information about the 8260 Fault Tolerant Controller module.

3.1 8260 Fault Tolerant Controller Module Overview

The controller module is an essential component of the 8260 and provides the following functions:

- Clock generating and its distribution across Enhanced TriChannel and ShuntBus

  This provides the clocking to the backplane and synchronizes the operation of all the installed modules.

- Monitoring the hub temperature and taking appropriate action in overheated conditions

  When the hub temperature rises in a particular area, the overheated condition is signaled to the controller module. Then, the controller module may power down 8260 modules within that area according to the power classes assigned to the modules. This will be done to bring down the temperature of the hub to an acceptable limit.

- Inventory and intelligent power management

  Each 8260 module has a serial EEPROM which is used for power management and inventory purposes. The EEPROM is programmed at manufacturing and includes information about how much power the module requires, its serial number, model number, the vendor ID, and its hardware revision level. Upon insertion into the hub, the 8260 modules will send Vital Product Data (VPD) and their power requirements over the control bus (SCI) to the controller module.

  The controller module also has knowledge of how many power supplies are installed in the hub and how much of the power is used by the currently installed modules; therefore, it is able to determine if there is enough power left in the hub to power up the new module. If the answer is yes, the controller module will apply full power to the module allowing it to operate normally. The controller module will also update its internal power tables to take into account the power consumption of the new module. Finally, the controller module informs the DMM of the VPD of the newly inserted module. Via the DMM command, you can also display information about the power supplies installed and the amount of power used by the existing modules. More details about the intelligent power subsystem and the role the controller module plays in managing the power for the hub is found in Chapter 5, “8260 Intelligent Power Management Subsystem” on page 73.

3.1.1 The Controller Module Front Panel

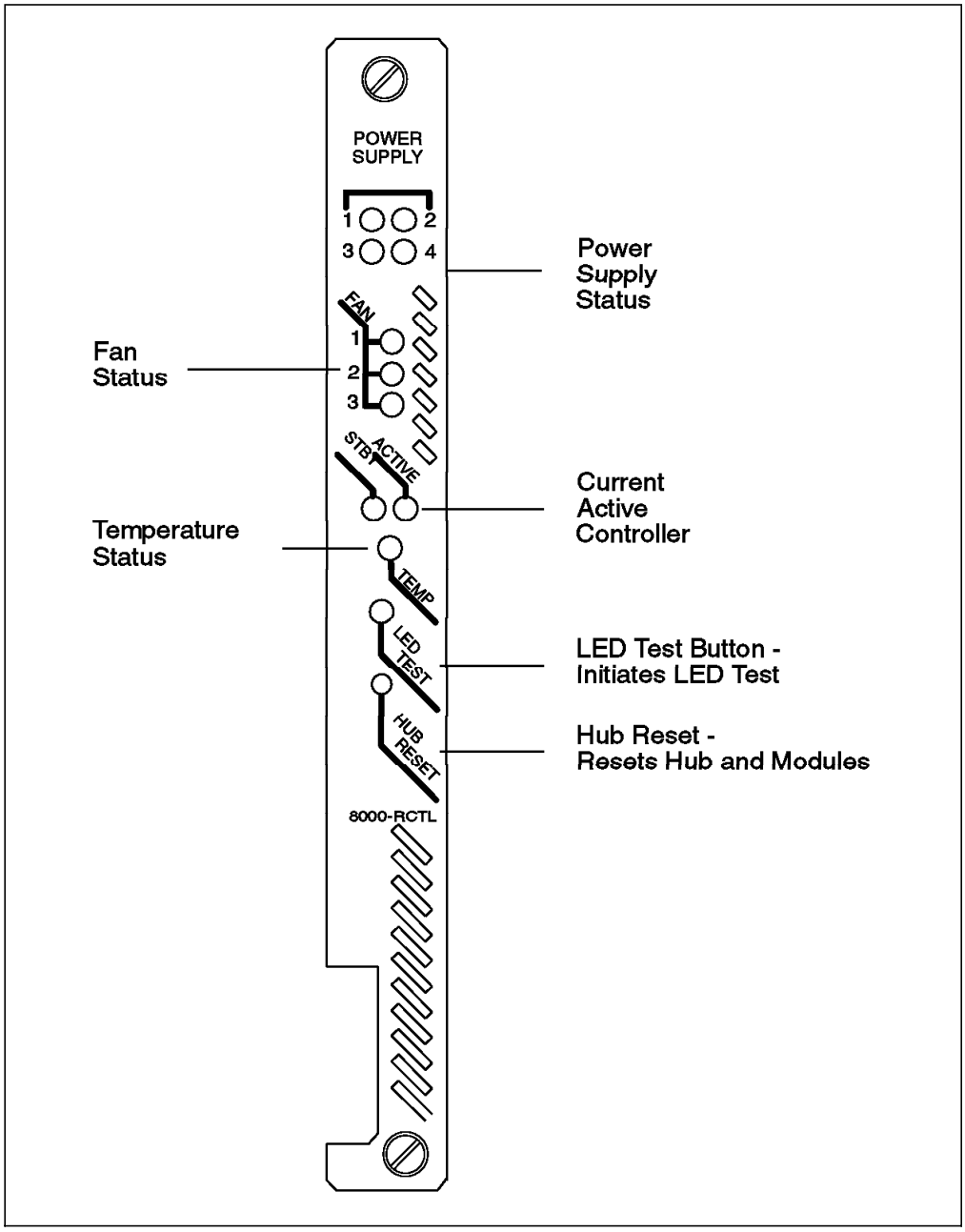


Figure 13. Front View of the Controller Module

Figure 13 shows the front view of the controller module.

Besides the hub reset and the LED test buttons, the controller module has 10 LEDs covering the 4 power supplies, 3 fans, active or standby mode and temperature on the front panel which indicate the state of the system environment. The names and locations of the buttons and LEDs are shown in Figure 13. The following table describes the meaning of the LEDs:

Table 3. 8260 controller Module LED Meaning		
LED	**STATE**	**Description**
Power Supply (1-4)	OFF	Power supply not present
	ON	Power supply operational
	Flashing	Power supply faulty
Fan (1-3)	OFF	LED has failed
	ON	FAN operational
	Flashing	FAN faulty
Temperature	OFF	Normal Temp
	Flashing	Temperature exceeds limit
Active	OFF	Controller module is in the standby mode
	ON	Controller module is the active controller
Standby	OFF	Controller module is the active controller
	ON	Controller module is the active controller
	Flashing	Controller module is faulty

Hub Reset Button

Pressing this button, which is active on the active controller module only, resets all installed modules including both active and standby controller modules.

If you issue the reset hub command at the 8260 console, it will give you the same result as using the hub reset button.

Note

Prior to resetting a hub, ensure that you save all parameter changes made; otherwise, you will have to re-enter them. Also remember that when the hub is reset, the network operation is disrupted.

LED Test Button

The LED test button is used to verify LED operation for all LEDs on all 8250 and 8260 modules installed. When you press the LED test button, every LED on every installed module should light up for approximately 5 seconds. Any LED that does not light is defective.

After 5 seconds, the port status LED will blink the number of times representative of the network to which that port is assigned for every port assigned to a backplane network. For example, the number of times an 8250 module port status LED can blink ranges from 1 to 7 for token-ring networks, from 1 to 3 for Ethernet networks and from 1 to 4 for FDDI networks. The port status LED display will last approximately 25 seconds.

For every port which is not assigned to a backplane network, the port status LED will turn off and remain off for approximately 25 seconds.

3.1.2 Controller Module Fault Tolerance

There are two dedicated slots, 18 and 19, provided for installing the controller module. Once installed, the controller does not need to be configured. Since the controller module is a critical component, it is recommended to have a second controller module installed in the hub for backup purposes.

When two controller modules are installed in the hub, one is active and the other will be a standby. Both the active and standby controller modules monitor and modify the hub operating conditions such as temperature and power. This redundant monitoring and control capability enables the standby controller module to be ready to take over from the active controller module should the active controller module fail.

When the standby controller module takes over from the active controller module, all the installed modules perform a fast reboot. Fast reboot results in all the 8260 modules equipped with onboard memory (NVRAM) to automatically load the configuration stored there. This occurs regardless of the current DIP switch settings on the modules. Fast reboot facilitates immediate resumption of the hub activity following the failure of the active controller module and takeover by the standby controller module. However, note that the takeover of the operation by the standby controller module is disruptive to the operation of the network and the users attached to the network.

Note: 8250 media modules do not have onboard memory to store configuration information. Therefore, following a reboot due to the failure of the active controller module, they will be configured by the DIP switch settings on the module (in an unmanaged hub) or via the configuration stored in the management module (in a managed hub).

If two controller modules are installed in a hub that is already powered up, the first controller module to be installed becomes the active controller module and the second controller module to be installed becomes the standby controller module. This is regardless of the slot in which the controller modules are installed. However, if two controller modules are installed in a hub that is not yet powered up, the controller module installed in slot 18 becomes the active controller module when the hub is subsequently powered up. Also, after a hub is reset due to power outage, pressing the reset button on the active controller module, or through 8260 DMM commands, the controller module in slot 18 becomes the active controller module and the controller module installed in slot 19 becomes the standby controller module.

3.1.3 Installing and Configuring the Fault Tolerant Controller Module

To install the controller module:

- Unpack the controller module from the shipping carton.
- Remove the blank faceplate from slot 18 and/or 19 depending on which slot is for installation.
- Insert the controller module into the top and bottom board guides and slide it into the hub until it is flush with the front of the hub.
- Tighten the two spring-loaded screws securely.

3.1.4 8260 Fault Tolerant Controller Module Considerations

- Up to two controller modules can be installed in the 8260 hub.
- Neither controller module occupies a payload slot.
- When 2 modules are installed, one is active and the other is standby.
- The hub reset button is only active on the active controller module.
- The LED test button is active on both active and standby controller modules.
- When a DMM is the active management module, the controller module will be seen in either slot 18 and/or 19.
- When an 8250 xMM is the active management module, the controller module will be seen in slot 17 although it physically resides in slot 18 and/or 19. As a result, when an 8250 management module is to be the master management module in the 8260, slot 17 must be empty or have the 8250 Right Boundary Adapter installed.
- When an 8250 xMM is the active management module, the standby controller module is invisible to the xMM. However, as soon as the standby controller module becomes the active controller module, it is then automatically seen by xMM to be in slot 17.
- When there is no DMM installed on the 8260 and an 8250 xMM is used as the master management module, one of the following levels of the xMM is required to identify the active controller module in slot 17:
  - EMM version 4.0 (or later)
  - TRMM version 2.1 (or later)
  - FMM version 2.0 (or later)
- The 8250 controller module can not be used in the 8260 hub.
- The 8260 controller module can not be used in the 8250 hub.
- One active controller module is always required to operate the 8260 hub.
- It is recommended to have a second controller module installed for redundancy.
- The switch over from the active controller module to the standby controller module is disruptive to the operation of the network.

Chapter 4. 8260 Distributed Management Architecture

This chapter will provide an in-depth look at the distributed management architecture of the 8260. The items we will cover are:

- 8260 distributed management architecture
- The Distributed Management Module (DMM)
- Ethernet Carrier - Distributed Management Module (EC-DMM)
- Ethernet Medium Access Carrier (E-MAC) daughter board
- Token-Ring Medium Access Carrier (T-MAC) daughter board
- Command overview
- Differences between using 8260 and 8250 management modules to manage the 8260

4.1 8260 Distributed Management Architecture

To fully manage the 8260 and the installed modules, the 8260 uses a distributed management architecture. In this architecture, the various tasks of managing the various elements of the hub are distributed across the following elements:

- Distributed management module
- MAC daughter cards
- Controller module

There are 2 types of distributed management module (DMM):

- Stand-alone DMM
  - The DMM is called a stand-alone card because it does not have any mounting facility for the daughter cards.
- EC-DMM
  - This module allows you to mount up to six Ethernet Medium Access Carrier (E-MAC) daughter cards on it. At the time of writing there is no carrier DMM available for mounting token-ring MAC (T-MAC) daughter cards.

In terms of management functions, DMM and EC-DMM are identical. The only difference between these two cards is their ability to house Ethernet MAC daughter cards. Therefore, as this section is discussing management in general, the term DMM will be used to refer to both 8260 management modules (stand-alone DMM and EC-DMM). In the next section we will look at the specific management modules and discuss their capabilities and their differences.

The DMM, along with the fault tolerant controller module, manages and controls the 8260 hub and its modules. However, to perform certain management functions such as network traffic monitoring, there is a need for a daughter card to assist the DMM. There are two types of daughter cards:

- Ethernet Medium Access Carrier (E-MAC) daughter card
- Token-ring Medium Access Carrier (T-MAC) daughter card

These daughter cards provide the following two functions:

- Interface to the backplane segments

  To be able to communicate with devices attached to any of the backplane segments, DMM requires an interface to that segment. The interface to the Ethernet segments on the backplane is provided to DMM via E-MAC, whereas T-MAC allows DMM to interface with the token-ring segments on the ShuntBus. Note that DMM requires one MAC daughter card for each network on the backplane thru which DMM is going to communicate with the other devices.

  DMM will use the interface to the backplane segments to communicate with the devices attached to these segments using IP. For example, to be able to manage the 8260 via an SNMP manager, DMM must have an interface to a network thru which the SNMP manager can be accessed.

- Network monitoring

  Daughter cards attach to the appropriate backplane segment (token-ring or Ethernet) and listen to the traffic flow and pass all the information back to DMM.

Note: Ethernet MAC daughter cards can be installed on EC-DMM or Ethernet media modules, whereas token-ring MAC daughter cards must always be installed on token-ring media modules.

The combination of DMM and daughter cards provides a cost efficient management architecture that consolidates media management into a single card, while distributing network monitoring across a series of protocol dependent daughter cards. The DMM is a generic (protocol independent) module that can be used for both in-band and out-of-band management. As mentioned above, when used for in-band management, DMM requires a daughter card. The flexibility and reduction in cost is achieved by distributing the network monitoring function to daughter cards which can be mounted on EC-DMM (E-MAC only) or media modules, so they do not use any valuable payload slots. This also means you only need one DMM to manage the entire 8260. If your network grows and you need to invest in more network monitoring function, you can install additional daughter card(s) matching the protocol of your new network(s) by just mounting them on the existing media module or EC-DMM (E-MAC only).

The MAC daughter cards will be assigned to the token-ring or Ethernet backplane using DMM commands. Once assigned to a backplane segment, they will be able to monitor the traffic on that segment and pass the collected information to the DMM. Note that the MAC daughter cards installed on the media modules will communicate with the DMM (or EC-DMM) using the MLAN, as shown in Figure 14 on page 37. The E-MACs installed on the EC-DMM, however, will use the onboard circuitry of the EC-DMM to communicate with DMM.

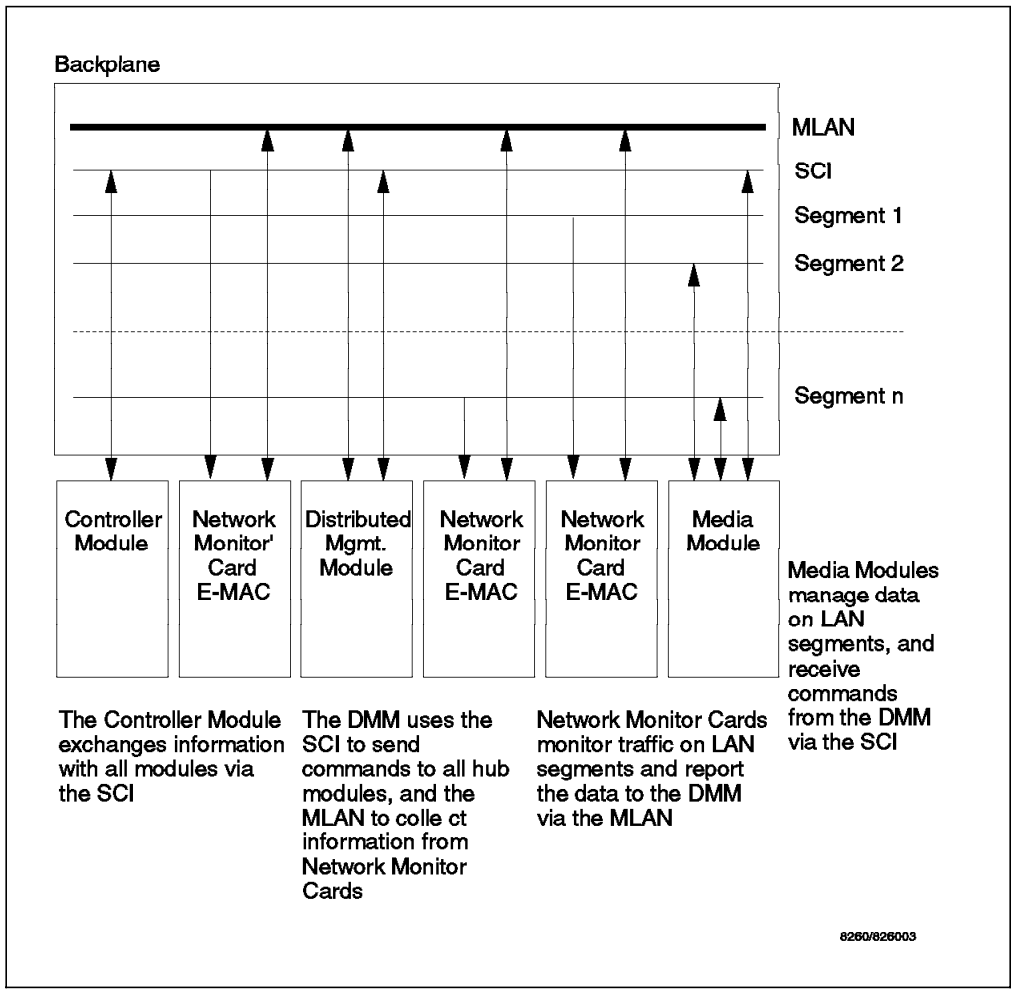


Figure 14. Management Schematic

The DMM (and daughter cards) provide management and control facilities in the following areas:

- **Configuration**

  The DMM, networks, modules, and port settings can be configured through the DMM using DMM commands. The DMM can be used to configure 8250 as well as 8260 modules.

- **Statistics and fault reporting**

  E-MAC and T-MAC provide support for collecting an extensive range of statistics based on RMON.

- **Out-of-band and in-band downloading**

  The DMM provides both in-band and out-of-band download features for downloading new software to DMM, media modules, and daughter cards. Trivial File Transfer Protocol (TFTP) is used for in-band downloads. Out-of-band downloads allow you to download software using the Xmodem protocol from a local or modem attached PC (with ASCII emulation software) attached to the RS-232 port on the front panel of the DMM.

- **SNMP support**

In a Simple Network Management Protocol (SNMP) managed environment the DMM acts as the SNMP agent, responding to SNMP requests and generating SNMP traps.

- **Telnet support**

  Using Telnet you can log in remotely to any DMM on the network and manage it from the remote station. You can also use Telnet from the terminal attached to the DMM to log in to any other device which supports Telnet.

- **Inventory**

  The DMM provides a complete inventory of the hub including power supplies, fans and modules installed in the 8260.

- **Staging**

  The media modules save their configuration information in an onboard non-volatile RAM (NVRAM). This means flexibility for network managers as they can configure the modules at a central site and then send them out to the remote locations for installation.

- **Power management**

  The DMM when used in conjunction with the fault tolerant controller module can be used to manage the power subsystem. For example, it can set power classes for modules and turn power fault tolerance on and off.

- **Mapping**

  DMM allows you to display a detailed topological ring map including address-to-port mapping about the token-ring segments on the network.

4.1.1 IP Addressing for DMM

Because of the centralized approach to management used in the 8260 there is a need for a new approach for assigning IP addresses to DMM when compared to the 8250. This is because, you may use a single DMM to communicate with IP stations attached to multiple different segments on the backplane.

The following is the summary of the steps you must take, in order to enable DMM to use IP to communicate with the other stations:

1. Assign an IP address to each of the networks on the backplane.
2. Assign an E-MAC or T-MAC to that network. This results in the T-MAC or E-MAC assuming the IP address of that network.
3. The DMM will now be able to communicate across that network using the IP address assigned to the T-MAC or E-MAC. In fact, DMM will send the IP packets over MLAN to the appropriate E-MAC or T-MAC and the E-MAC or T-MAC will forward it over the segment to which it is attached.

   Note: A single DMM can communicate across multiple backplane segments as long as there is a daughter card assigned to each of those backplane segment.

4.2 The Distributed Management Module (DMM)

The stand-alone DMM is a single-slot management module that has no facility for carrying daughter cards.

The DMM has 1 module status LED, a 4-character display with a display control toggle button and 2 serial port connectors as shown in Figure 15.

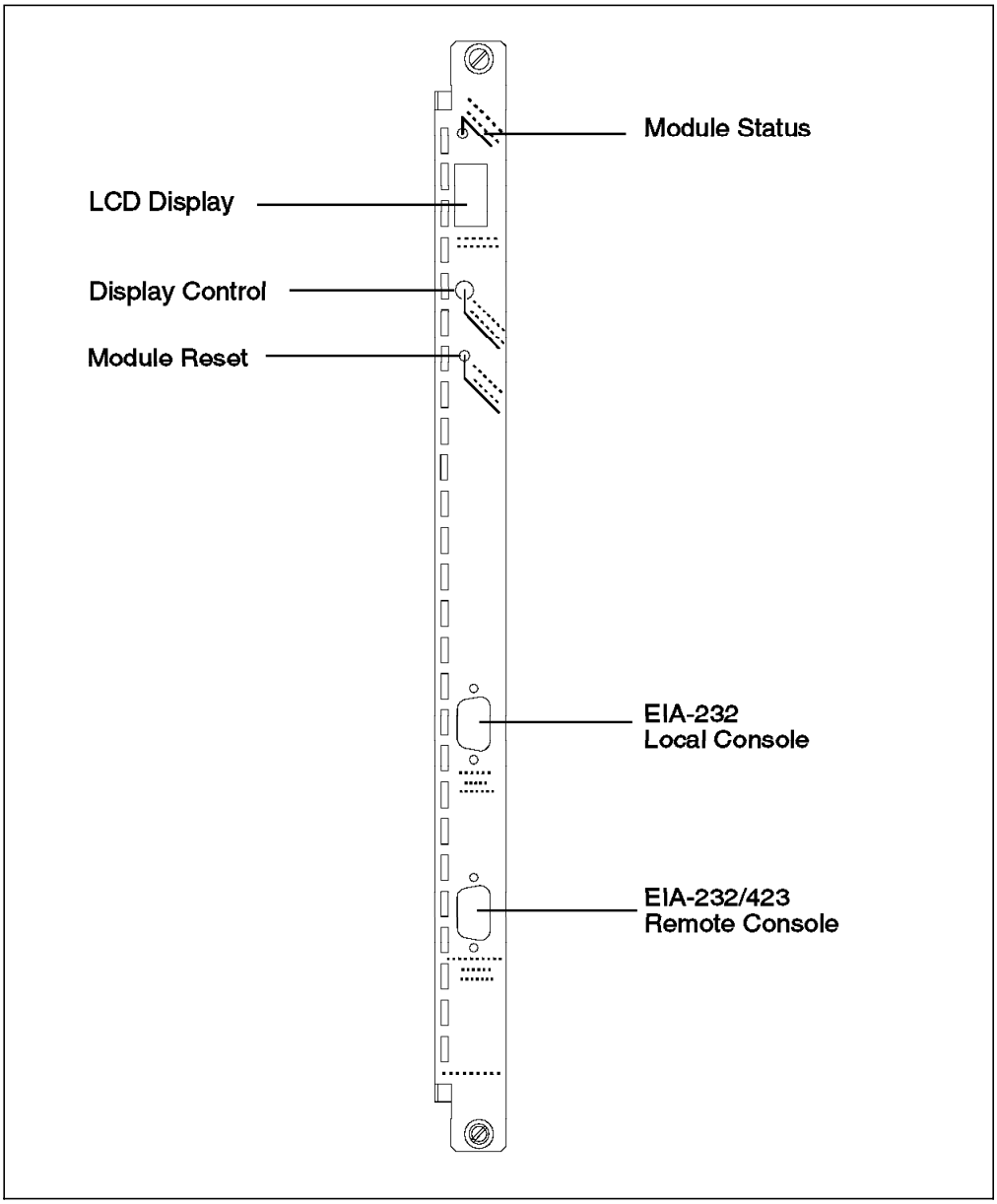


Figure 15. DMM Front Panel

4.2.1 Unpacking and Installing the DMM

Caution

As always, great care should be taken when handling logic cards. The level of static electricity that can build up in the human body can be thousands of times greater than the very small switching voltage used in logic cards. An analogy would be connecting your Hi-Fi or TV set to 10,000 volts. It wouldn't last long!

Remove the card from its shipping container and check it for damage.
There are 2 jumper blocks that may need to be changed. Namely, JP8 and JP9 as shown in Figure 16. These jumpers allow you to set the auxiliary DB-9 connector to RS-232 or RS-423. For the factory default, which is RS-232, the jumper will be between pins 2 and 3 (the bottom 2 pins) of JP8. To select RS-423 mode, the jumper on JP8 should be changed to pins 1 and 2 (the upper pins). For RS-423, the jumper MUST be installed on JP9. For RS-232, remove the jumper from JP9.

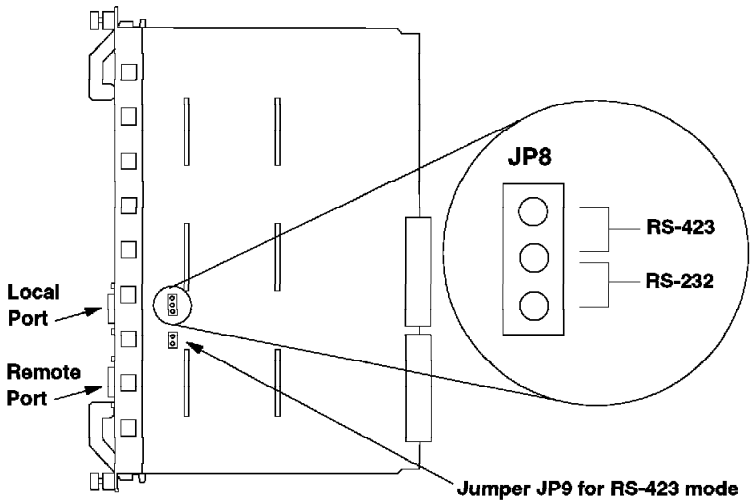


Figure 16. Jumpering for the DMM DB-9 Ports

Holding the DMM by the faceplate, slide it into the slot in the 8260. Like all 8260 modules it can be hot plugged.

If the DMM has been installed correctly and is functioning the status LED should come on. The LCD display should show *diag* then either *rdy* for the master module or *stby* for a backup module.

4.2.2 DMM LED Indicators

Table 4 on page 41 shows the meaning of the status LED.

Table 4. DMM Status LED			
LED name	**Color**	**State**	**Indicates**
Status	Green	OFF	Power off or module failure
		ON	Power on and software functioning properly
		Blinking	Power on but diagnostics have failed

The LCD display and display control button are used to:

- Display the current operating state of the module
- Determine the network assignment of ports and 8260 modules in the hub
- Display the version of the DMM microcode

The LCD display normally shows the module operating state. To display the DMM microcode version, press the button until the display reads *Vers*, and one second after releasing the button the version will be displayed. Table 5 shows the possible states of the display.

Table 5. DMM LCD Display	
Display	**Definition**
Diag	The DMM is running diagnostics
Rdy	The DMM is the active (master) management module
Stby	The DMM is in standby mode
Dnld	New microcode is being downloaded
Vers	Microcode level of the DMM
LED	Displays when the controller LED test button is pressed

4.2.3 Console and Auxiliary Ports

There are two DB-9 ports on the faceplate of the DMM. The upper port is called the *console* port and is used for attaching a terminal locally (or via a modem) to the DMM. This terminal is used to provide out-of-band management capability for the 8260. See Table 6 for pinout of the cable used for attaching terminals to this port.

Table 6. Console Port Pinouts	
Pin #	**Signal Name**
1	Carrier detect (CD)
2	Receive data (RX)
3	Transmit Data (TX)
4	Data terminal ready (DTR)
5	Signal ground (SG)
6	Data set ready (DSR)
7	Request to send (RTS)
8	Clear to send (CTS)
9	No connection

The lower port is the *auxiliary* port and can be jumpered for RS-232 or RS-423 operation. This port allows you to attach a terminal locally (or via modem) to DMM. Note: The default is RS-232. See Table 7 on page 42 for the pinout of the cables used for attaching terminals to the auxiliary port.

Table 7. Auxiliary Port Pinouts

Pin #	Signal Name
1	Carrier detect (CD)
2	Receive data plus (RX+)
3	Transmit Data (TX)
4	Data terminal ready (DTR)
5	Signal ground (SG)
6	Data set ready (DSR)
7	Request to send (RTS)
8	Clear to send (CTS)
9	Receive Data Minus (RX-) if RS-423, otherwise no connection

Note

You can attach terminals to both the console and auxiliary port at the same time, and both of them will be able to access the DMM simultaneously.

4.2.3.1 Modems for Connecting Terminals to DMM

The console port and auxiliary port can be used to connect a modem for remote dial-in. The following requirements must be met:

1. The modem must be 100% Hayes compatible.
2. Any of the following baud rates may be used:

   300, 1200, 2400, 9600, 19,200 or 38,400
3. The modem must be placed in Dumb/Auto Answer mode. This can be done by entering the commands listed in Table 8 from a terminal directly attached to the modem.

Table 8. Commands Required to Set Up the Modem for the Console Port

Commands #	Definition
at&f [enter]	Restore factory defaults
at&d0 [enter]	Ignore changes in DTR status **
ats0=1 [enter]	Auto-answer on first ring
ats0? [enter]	Verify Auto-answer (should return 001
atq1 [enter]	Does not return result codes
at&W [enter]	Save this configuration
at&Y [enter]	Define this configuration as the default
at&d2 [enter]	Indicates hangup and assumes command state when an On to Off transition of DTR occurs **

** If you issue the *Set Terminal Hangup Enable* command for modem use, you must change the DTR parameter as defined by the ″at&d2″ command to ensure

proper modem operation. See 4.2.4.3, “Configuring Terminal Settings for DMM” on page 47 for description of Set Terminal Hangup command.

4.2.4 Configuring the DMM

The following table is a quick reference to the tasks required to configure the DMM interface.

Table 9. DMM Interface Configuration Quick Reference

Procedure	**Command**
Configure the terminal to match default DMM settings	Refer to the documentation provided with the terminal
Configure DMM users	SET LOGIN USER SET LOGIN ADMINISTRATOR SET LOGIN SUPERUSER SET LOGIN PASSWORD SET LOGIN ACCESS
Configure DMM terminal settings	SET TERMINAL CONSOLE SET TERMINAL AUXILIARY SET TERMINAL PROMPT SET TERMINAL TIMEOUT
Hub configuration	SET CLOCK
Device configuration	SET DEVICE NAME SET DEVICE LOCATION SET DEVICE CONATCT SET DEVICE DIAGNOSTICS SET DEVICE MAC_ADDR_ORDER SET DEVICE RESET_MASTERSHIP SET DEVICE DIP_CONFIGURATION SET DEVICE TRAP_RECEIVER
IP configuration	SET IP IP_ADDRESS SET IP DEFAULT_GATEWAY SET IP SUBNET_MASK SET IP ACTIVE_DEFAULT_GATEWAY
SNMP configuration	SET COMMUNITY SET ALERT AUTHENTICATION SET ALERT CHANGE SET ALERT CONSOLE_DISPLAY SET ALERT HELLO SET ALERT PORT_UP_DOWN SET ALERT SCRIPT

Before your terminal and the DMM can communicate you must set up the terminal parameters to match the DMM settings. The factory defaults and options for the DMM are listed in Table 10. Initially the terminal must match the defaults.

Table 10 (Page 1 of 2). DMM Terminal Defaults and Options

Parameter	**Factory Default**	**Options**
Baud	9600	300,1200,2400,4800,9600,19200,38400
Data bits	8	7 or 8
Parity	None	Odd, Even or None

Table 10 (Page 2 of 2). DMM Terminal Defaults and Options		
Parameter	**Factory Default**	**Options**
Stop Bits	1	1 or 2

Once the terminal has been configured press the Enter key. If the terminal has been configured correctly the following message should be displayed:

```
8260A

Distributed Management Module (v2.10-H)


Login:
```

Figure 17. DMM Login Message

To log in as *superuser* at the *Login* prompt type in *system* and press the Enter key. The module is shipped from the factory with a null password, so at the *Password* prompt press Enter.

At this stage you are logged into the 8260 with full access to all commands.

4.2.4.1 Configuring DMM Users

Three types of users can be used to access DMM:

- *User*

  This type of user can view the configuration of the 8260 and all the installed modules and daughter cards. Additionally, this user can obtain statistics about the various components of the network.

- *Administrator*

  This type of user can perform all the user functions. Additionally, this user can modify the configuration of the hub and all the installed modules and daughter cards.

- *Superuser*

  This type of user can perform all the functions of the administrator. Additionally, this user can create new users and perform maintenance functions such as downloading new software to the DMM and other modules.

The DMM is shipped from the factory with a single user defined. This user is called *system* and has superuser access. Also, it does not have any password assigned to it.

After logging in to DMM for the first time, it is strongly advised that for security reasons you change the password for the superuser using the example given in Figure 18 on page 45.

```
8260A> set login password

Enter current session password for user "system":

Enter new password:
Verify - re-enter password:

User password changed.
8260A>
```

Figure 18. Changing Superuser Password

Note: DMM passwords are case sensitive.

You may define new login names with user, administrator and superuser authority. Figure 19 shows an example of how to define a new superuser.

```
8260A> set login super_user
Confirm with Carriage Return

8260A> set login super_user

Enter current session password for user "system":


Enter Login Name: shabani

Enter Login Password: [new password]
Verify - re-enter password: [new password]

Login successfully entered.
Login account will not be activated until it is saved.
8260A>
```

Figure 19. Defining New DMM Superuser

Defining the other user types is identical to defining superuser, except that in the set command you must specify *user* or *administrator* as the user type.

You can display the current users defined in your DMM, using the following command:

```
8260A> show login
```

An example of the output from this command is shown in Figure 20 on page 46.

```
8260A> show login

Login Table:

        Index   Login Name       Access          Active Sessions
        -----   --------------   -------------   ---------------
            1   system           Super User            1
            2   shabani          Super User            0
            3   admin1           Administrator         0
            4   user1            User                  0
            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 00:15:27

8260A>
```

Figure 20. Display of Defined DMM Users

A superuser can delete entries for other users with the following command:

```
8260A> clear login {index | all}
```

Where *index* is as shown in Figure 20.

There can be up to a maximum of 10 users (any combination) defined in a DMM. However, at any point in time, there can be only one user with write access (administrator or superuser) logged in to a DMM. Therefore, if you try to log in to DMM as an administrator or superuser, when there is already an administrator (or a superuser) logged in to that DMM, you will be given a user access. However, a superuser who is granted a user access in this way, can use the example shown in Figure 21 on page 47 to force the termination of the current session which has the write access (currently logged in administrator or another superuser) and obtain the superuser access to DMM.

```
Login:
Login: system
Password:

A user with Super User or Administrator Access is already logged in.
You are being logged in with User Access ...


Welcome to user service on 8260A.
8260A> set login access super_user


Super_user access granted.

8260A>
```

Figure 21. Forced Termination of Existing DMM Users

In this example, we tried to log in as a superuser and since there was already an administrator logged in, we got a user access. After issuing the ″set login access″ command, the administrator user was logged off and our user acquired the superuser authorization.

4.2.4.2 Resetting Superuser Password to Factory Default

If you forget the superuser password for DMM, you may use the following procedure to reset the password to factory default:

- Try to log in to DMM using the superuser ID.
- When prompted for the password, enter *force*.
- Your login request will be rejected and you will be prompted to enter the user ID again. This time, enter *force* as the user ID.
- When prompted for the password, enter *force*.
- Immediately press the *reset* button on the DMM.

Note that the above procedure will result in the following:

- Restores the ″system″ password to nulls.
- Resets DEVICE and TERMINAL settings to factory default.
- All the other LOGIN entries, other than SYSTEM are cleared.

4.2.4.3 Configuring Terminal Settings for DMM

The DMM provides the following commands to allow you to customize your terminal connection:

- **Set Terminal Console**

  This command allows you to set the following communications parameters for the DMM to communicate with your terminal:

  – Baud

    This parameter allows you to set the baud rate at which the DMM will send and receive data. For example, the following allows you to change the baud rate to 9600.

    `8260> set terminal console baud 9600`

Note: The baud rate specified in this command must match the settings of your terminal; otherwise, after issuing this command, the communication between the terminal and DMM will be lost. In that case, you must change the setting of your terminal before you can reestablish the communication.

– Data_bits

  This parameter allows you to set the number of data bits used by DMM for communication with your terminal. The following command allows you to change the number of data bits to 8.

  ```
  8260> set terminal console data_bits 8
  ```

  Note: The number of data bits specified in this command must match the settings of your terminal; otherwise, after issuing this command, the communication between the terminal and DMM will be lost. In that case, you must change the setting of your terminal before you can reestablish the communication.

– Stop_bits

  This parameter allows you to set the number of stop bits used for communication between your terminal and the DMM port. The following command allows you to change the number of stop bits to 2.

  ```
  8260> set terminal console stop_bits 2
  ```

– Parity

  This parameter allows you to set the parity setting used by DMM for communication with your terminal. For example, the following command allows you to change parity for DMM to even:

  ```
  8260> set terminal console parity even
  ```

  Note: The parity setting specified in this command must match the settings of your terminal; otherwise, after issuing this command, the communication between the terminal and DMM will be lost. In that case, you must change the setting of your terminal before you can reestablish the communication.

– Mode

  This command allows you to select which one of the following methods will be used by the DMM to communicate with the device attached to its port:

  - Command-line parser

    This setting allows DMM to communicate with a direct or modem attached device emulating an ASCII terminal. To use the command-line parser on the DMM port, you must issue the following command:

    ```
    8260A> set terminal console mode command_line
    ```

  - Serial Line Interface (SLIP)

    This setting allows DMM to use SLIP to communicate with a TCP/IP station attached to its port console or auxiliary port. An example of the command to set the SLIP interface on the DMM port, is given below:

    ```
    8260> set terminal console mode slip 9.67.46.3
    ```

In this example, 9.67.46.3 is the address of the TCP/IP station attached to the DMM port.

To use SLIP, you must also perform the following tasks:

1. Assign an IP address to DMM for communication over the SLIP interface. The following example defines 9.67.46.1 as the address used by DMM over the SLIP interface:

   ```
   8260> set ip ip_address 9.67.46.1 slip
   ```

2. Assign an IP subnet mask to be used by DMM for communication over the SLIP interface. The following example defines 255.255.255.240 as the subnet mask used by DMM over the SLIP interface:

   ```
   8260> set ip ip_address ff.ff.ff.f0 slip
   ```

3. Define the default gateway to be used by DMM for communication over the SLIP interface. The following example defines 9.67.46.2 as the default gateway used by DMM over the SLIP interface.

   ```
   8260> set ip default_gateway 9.67.46.2 slip
   ```

An example of using the SLIP setting is when the workstation attached to the DMM port is a TCP/IP station running a network management application which allows you to manage DMM using SNMP.

– Terminal_type

This command allows you to set the terminal type which will be used by DMM for establishing Telnet sessions. An example of this command is as follows:

```
8260> set terminal console terminal_type vt100
```

The terminal type set by this command is sent by DMM to the remote device when you establish a Telnet session from DMM to the remote device. This enables the remote device to send the proper control sequence for communication with DMM.

– Hangup

This command allows you to configure DMM to automatically hang up the modem (drop DTR) once you log out of the DMM. To do so, you must issue the following command:

```
8260> set terminal console hangup enable
```

The default is *disable* which means the modem will not hangup and an unauthorized user may pick up the last login session.

Note: You can specify the same parameters for the auxiliary port. All you need to do is replace *console* with *auxiliary* in the example commands given above.

- **Set Terminal Prompt**

This command enables you to customize the prompt displayed by DMM when you are connected to that DMM. An example of this command is as follows:

```
8260> set terminal prompt 8260A>
```

This option is very useful in identifying the DMM to which you are logged in. The default prompt is ″8260>″. It is recommended that you use the same ID for both the terminal prompt and the DMM device name. See 4.2.4.4, “ Configuring DMM Device” on page 50 for how to configure DMM device name.

- **Set Terminal Timeout**

  This command is used to specify the amount of time the terminal will remain active during the absence of keyboard activity. This command is used for security, to ensure that an unattended DMM console will not remain logged in for long periods. The default is ″0″ which means the terminal will never timeout. An example of this command is as follows:

  ```
  8260A> set terminal timeout 10
  ```

  Note that the value specified in the above command is in minutes.

You can display the current settings for console and auxiliary port using the following command:

```
8260> show terminal
```

An example of the output displayed by this command is shown in Figure 22.

```
Terminal Session Parameters:
  Prompt:       8260A>
  Timeout time: 0

Console Port Parameters:
  Baud:         9600
  Data bits:    8
  Parity:       NONE
  Stop bits:    2
  Hangup:       ENABLED
  Mode:         COMMAND LINE
  Terminal:     VT100

Auxiliary Port Parameters:
  Baud:         9600
  Data bits:    8
  Parity:       NONE
  Stop bits:    2
  Hangup:       DISABLED
  Mode:         SLIP     Destination IP Address: 9.67.46.3
  Terminal:     VT100

8260>
```

Figure 22. Output from Show Terminal Command

4.2.4.4 Configuring DMM Device

The following commands are used to allow you to configure the DMM:

- **Set Clock**

  This command allows you to set the time, day and date for the DMM. The following is an example of using this command:

  ```
  8260> set clock 15:45 95/1/19 Thursday
  ```

This command sets the clock to 3:45 p.m., Thursday, Jan 19th, 1995. The clock is driven by an internal battery which is designed to last for 10 years.

- **Set Device**

  This command allows you to configure the following for DMM:

  – Device name

    This command allows you to configure a name for DMM. It is recommended that each DMM in the network be assigned a unique name. The name can be a maximum of 31 characters long. It is a good idea to make sure that the name of the DMM and the prompt of the terminal which is directly attached to it match each other.

    The following command assigns the device name of *8260A* to this DMM:

```
8260> set device name
> Enter device name:
> 8260A
Device name changed.
8260A>
```

Figure 23. Set Device Name Command for DMM

  – Device location

    This command allows you to describe the location of the 8260 in which this DMM is installed. An example of this command is as follows:

```
8260A> set device location
Enter one line of text:
> ITSO LAB, Building 657, Raleigh

Location changed.
8260A>
```

Figure 24. Set Device Location Command for DMM

    Note that you can enter up to 78 alphanumeric characters to specify the location of the DMM.

  – Device contact

    This command allows you to specify the name of the person responsible for maintaining the 8260 in which this DMM is installed. An example of this command is as follows:

```
8260A> set device contact
Enter one line of text:
> Mohammad Shabani, 301-2339

Contact changed.
8260A>
```

Figure 25. Set Device Contact Command for DMM

    Note that you can enter up to 78 alphanumeric characters to specify the contact name for the DMM.

  – Device diagnostics

The factory default is for the DMM to run through a full set of diagnostics each time it is rebooted. By using the following command you can make the DMM bypass the diagnostics and boot up faster:

```
8260A> set device diagnostics disable
```

– MAC address order

In general, Ethernet devices uses canonical address format, whereas token-ring devices use a non-canonical address format. However, DMM is shipped from the factory to display all the addresses in canonical format regardless of the type of originating station. For example, with canonical setting for DMM, if we display the current ARP table entries of DMM, the result will be as shown in Figure 26.

```
8260A> show ip arp_cache

IP ARP Cache :

Interface   Address          Physical Address
---------   ---------        ----------------

   4        9.67.46.46       08-00-5a-13-39-6f
   5        9.67.46.237      02-00-00-c0-cc-6c
   5        9.67.46.238      08-00-5a-13-55-93

8260A>
```

Figure 26. Output from Show ARP_Cache Command with Canonical Setting

In this example 9.67.46.46 is an Ethernet attached station whereas 9.67.46.237, and 9.67.46.238 are both token-ring attached stations. As can be seen, all the addresses are shown in canonical format.

You may use the following command to set the non-canonical format to be used by DMM:

```
8260A> set device mac_addr_order noncanonical
```

After issuing the above command, the current ARP table will be displayed as shown in Figure 27.

```
8260A> show ip arp_cache

IP ARP Cache :

Interface   Address          Physical Address
---------   ---------        ----------------
0
   4        9.67.46.46       10-00-5a-c8-9c-f6
   5        9.67.46.237      40-00-00-03-33-36
   5        9.67.46.238      10-00-5a-c8-aa-c9

8260A>
```

Figure 27. Output from Show ARP_Cache Command with Non-Canonical Setting

You may use this command to set the address format used by DMM to be the same as the address format that you are most accustomed to.

– Reset mastership

You can configure DMM to force a mastership election when it is inserted into a hub. This option may be used to ensure that the DMM gets the opportunity to obtain the appropriate authority after it is removed and inserted back into the hub. The command to enable the forcing of mastership is as follows:

```
8260A> set device reset_mastership enable
```

– DIP configuration

  Each 8260 media module has a set of DIP switches which allow you to configure how the module should operate. Also, each module has a non-volatile RAM which is used to store the configuration information that you set for the module via DMM commands. This configuration information is sent by DMM to the module when the module is installed in the hub.

  Once installed, the 8260 module will be configured according to the following procedure:

  - The 8260 module attempts to configure itself from either its DIP switch settings or the onboard NVRAM. The setting of one of the DIP switches on the module determines if the module should try to use its DIP switch settings or the onboard NVRAM.
  - If a Master DMM is installed, the requested configuration is submitted for approval:
    - If the DMM has a saved configuration for module/slot, it overrides the requested configuration.
    - If the DMM does not have a saved configuration for the module/slot, it checks the requested configuration for validity:
      – If valid, the requested configuration is used.
      – If not valid, or DIP switches are used, the module is isolated and ports are disabled.
  - If no Master DMM is installed, the module tests the requested configuration for validity:
    - If valid, the requested configuration is used.
    - If not valid, or not present (NVRAM selected, but has no configuration), the module is isolated and ports are disabled.

  The above procedure will happen if you have issued the following command:

  ```
  8260A> set device dip_configuration disable
  ```

  However, you may configure your hub to bypass the above procedure and force the DIP switch settings on the module to be used all the time. To do so, you must issue the following command:

  ```
  8260A> set device dip_configuration enable
  ```

– Trap receiver

  You can enable DMM to receive traps from the other SNMP devices (such as other 8260 hubs) in your network. To do so, you must issue the following command:

  ```
  8260A> set device trap_receiver enable
  ```

Note that for your DMM to receive traps from the other stations, your DMM must be defined as a trap receiver in the community table of the other stations.

After setting all the parameters for DMM you must ensure that you save them using the following command:

```
8260A> save device
```

You can display the current device settings for DMM using the following command:

```
8260A> show device
```

An example of the output from this command is shown in Figure 28.

```
8260A> show device

IBM 8260 Distributed Management Module (DMM) v2.10-H  pSOS+  SNMP

Name:  8260A
Location:
  ITSO LAB, Building 657, Raleigh
For assistance contact:
  Mohammad Shabani, 301-2339

Operational Version: v2.10-H       Boot Version:  v1.01

Serial Number: 1067067             Service Date:  94/04/21    Restarts: 59

Dip Configuration: DISABLED        Diagnostics:  DISABLED
Reset Mastership:  ENABLED         Trap Receive: ENABLED
MAC Address Order: NONCANONICAL

8260A>
```

Figure 28. Output from Show Device Command

4.2.4.5 Configuring DMM IP Parameters

As mentioned earlier in this chapter, DMM will use the IP stack provided by T-MAC and E-MAC to communicate with the other IP stations. For DMM to use the IP stack of E-MAC and T-MAC, you must first perform the following tasks:

1. Assign the following parameter for one or more of the backplane segments:
   - IP address

     For example, to assign an IP address of 9.67.46.235 to the token_ring_10 segment on the ShuntBus, you must use the following command:

     ```
     8260A> set ip ip_address 9.67.46.235 token_ring_10
     ```

   - Subnet mask

     For example, to assign a subnet mask of 255.255.255.240 to the token_ring_10 segment on the ShuntBus, you must use the following command:

     ```
     8260A> set ip subnet_mask ff.ff.ff.f0 token_ring_10
     ```

   - Default gateway

For example, to assign a default gateway of 9.67.46.238 to the token_ring_10 segment on the ShuntBus, you must use the following command:

```
8260A> set ip default_gateway 9.67.46.238 token_ring_10
```

Note that DMM will use the IP address assigned to a segment to communicate through that segment. Therefore, if you have assigned IP addresses to more than one backplane segment, your DMM, effectively, has multiple addresses (one in each segment).

You can display the IP parameters which are currently assigned in your 8260, using the following command:

```
8260A> show ip
```

An example of the output from this command is shown in Figure 29.

```
8260A> show ip

 Active Default Gateway : 127.0.0.1

 Operational Active Default Gateway : 9.67.46.46

Index  Network       Slot  IP Address       Subnet Mask      Default Gateway
-----  ------------- ----  -----------      -----------      ---------------

  1    ETHERNET_1    N/A   9.67.46.41       ff.ff.ff.f0      9.67.46.46
  2    TOKEN_RING_10 N/A   9.67.46.235      ff.ff.ff.f0      9.67.46.238
  3    SLIP          N/A   9.67.46.1        ff.ff.ff.f0      9.67.46.2

8260A>
```

Figure 29. Output from Show IP Command

In this example, our DMM is assigned three IP addresses:

- 9.67.46.1 for slip connection through the console/auxiliary port
- 9.67.46.46 for connection through Ethernet_1
- 9.67.46.238 for connection through token_ring_10

You can clear any of the IP entries assigned to DMM using the following command:

```
8260A> clear ip index
```

Where *index* is the number of the network shown in Figure 29.

2. When there are multiple default gateways defined, you may select one gateway, known as the active default gateway, that will be used by DMM to send the packets to unknown destinations. You can use the following command to select the active default gateway:

   ```
   8260A> set ip active_default_gateway 9.67.46.238
   ```

   If you do not select the active default gateway, by default, the active default gateway is the default gateway assigned to the first interface that you have assigned to your DMM. For example, for the DMM shown in Figure 29, the active default gateway would have been 9.67.46.46 had we not defined 9.67.46.238 as the active default gateway.

3. After configuring the IP address(es) for DMM, you must assign an E-MAC or T-MAC to any backplane through which the DMM is going to communicate using IP. For information about how to assign E-MAC or T-MAC to a backplane segment, please refer to 4.4, “MAC Daughter Cards” on page 61.

4.2.4.6 Configuring DMM SNMP Parameters

The DMM acts as an agent in an SNMP managed environment, enabling you to manage the 8260 using an SNMP manager. The DMM supports SNMP by responding to SNMP requests from the SNMP managers and generating SNMP traps which can be sent to SNMP managers.

There is a community table in DMM which allows you to define the IP address and community name of up to 10 SNMP managers. Each of these SNMP managers can have one of the following attributes assigned to it:

- *Read only*

  Allows the specified SNMP manager to read SNMP variables via the GET command.

- *Read-write*

  Allows the specified SNMP manager to read and write SNMP variables via the GET and SET commands.

- *Trap*

  Enables DMM to send traps to the specified SNMP manager.

- *Read trap*

  Allows the specified SNMP manager to read SNMP variables and receive traps.

- *All*

  Allows the SNMP manager to read SNMP variables, change the variables via the SET command and receive traps from DMM.

The following command is an example of how to define an SNMP manager *9.67.46.45* with the community name of *public* to be able to perform *all* functions:

```
8260A> set community public 9.67.46.45 all
```

You can display the contents of the community name using the following command:

```
8260A> show community
```

An example of the output from this command is shown in Figure 30 on page 57.

```
8260A> show community

        Index  Community Name        IP Address       Access
        -----  --------------------  ---------------  ------
            1  public                ***.***.***.***  Read-Only
            2  public                9.24.104.23      All
            3  public                9.24.104.70      All
            4  public                9.67.46.45       All
            5  [empty]
            6  [empty]
            7  [empty]
            8  [empty]
            9  [empty]
           10  [empty]

8260A>
```

Figure 30. Output from Show Community Command

You can clear entries from the community table using the following command:

```
8260A> clear community index
```

Where *index* is the number of the entry as shown in Figure 30.

DMM sends alerts (traps) when certain events occur. You can use the SET ALERT command to enable/disable specific alert features. These alert features are:

- *Authentication*

  DMM sends an alert when an unauthorized access is attempted to DMM using SNMP. You can enable DMM to send authentication traps using the following command:

  ```
  8260A> set alert authentication enable
  ```

- *Change*

  Any configuration change made in the hub results in DMM sending an alert. You can enable DMM to send change traps using the following command:

  ```
  8260A> set alert change enable
  ```

- *Hello*

  When DMM is activated, it sends one Hello trap every minute, 255 times until a valid SNMP message is received. You can enable DMM to send Hello traps using the following command:

  ```
  8260A> set alert hello enable
  ```

- *Console_display*

  Allows you to enable trap display on the local console attached to DMM. You can enable DMM to display traps on the local console using the following command:

  ```
  8260A> set alert console_display enable
  ```

- *Port_filter*

  Allows you to filter out unwanted port up/down messages on the local console. To set the port_filter alert you can use the following command:

```
8260A> set alert port_up_down {enable|disable|filter}
```

If you enable this option, all the port up and port down traps will be sent to the local console. “disable,” prevents the traps from being displayed on the local console. “filter” allows DMM to check the ALERT_FILTER setting for each port for displaying/suppressing the port up and port down alters. The ALERT_FILTER for each port can be set using the following example:

```
8260A> set port 2.1 alter_filter {enable|disable}
```

4.3 The EC-DMM (Ethernet Carrier - Distributed Management Module)

The EC-DMM is a single-slot management module that has the mounting ability to carry up to 6 Ethernet MAC daughter cards.

The EC-DMM has 1 module status LED, a 4-character display with a display control toggle switch, 24 Ethernet network status LEDs and 2 serial port connectors. Figure 31 on page 59 shows the layout of the DMM front panel.

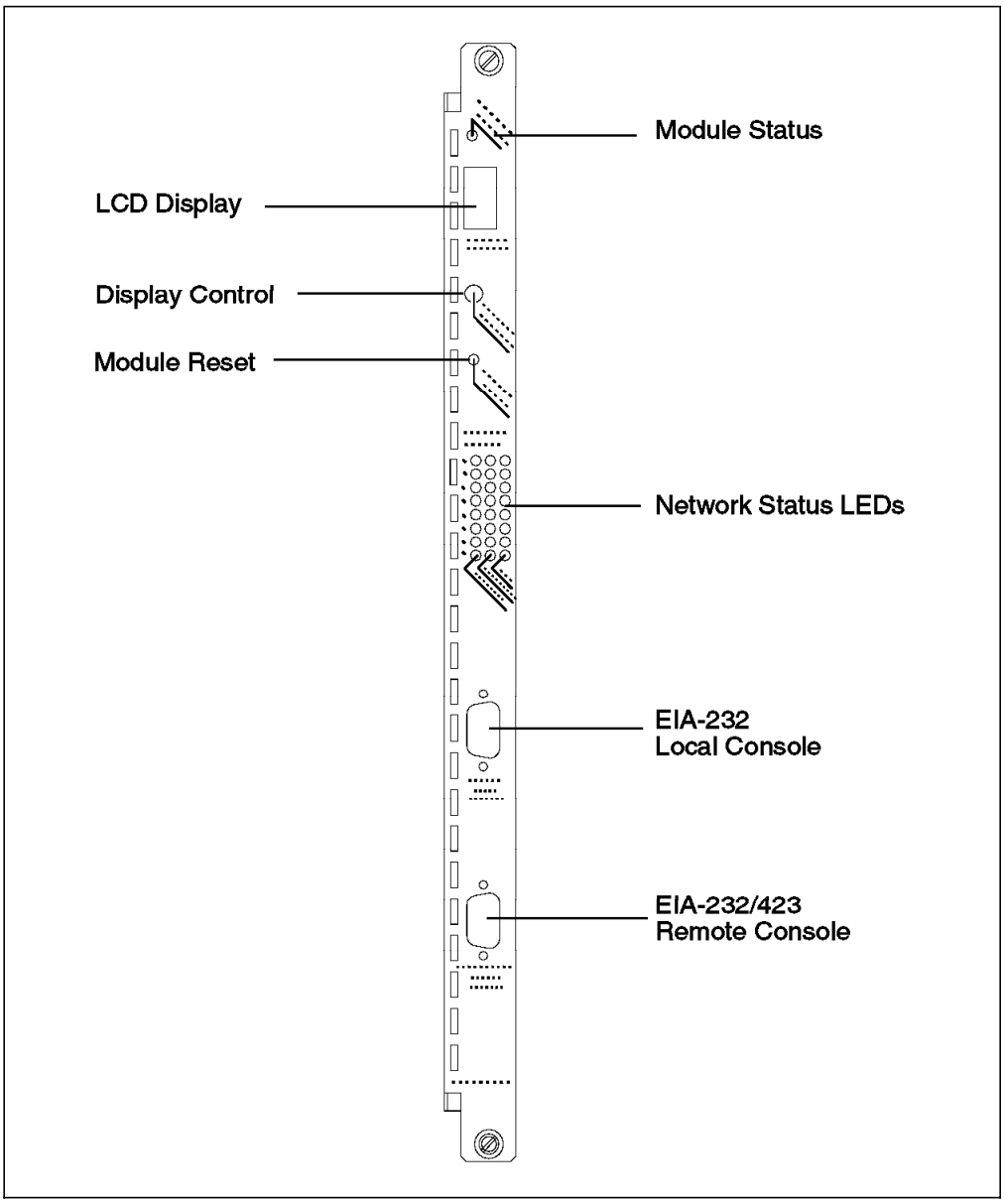


Figure 31. EC-DMM Front Panel

4.3.1 Installing the EC-DMM

Remove the card from its shipping container and check it for damage.
There are 2 jumper blocks that may need to be changed, JP8 and JP9. These jumpers are shown in Figure 32 on page 60. These jumpers allow you to set the auxiliary DB-9 connector to RS-232 or RS-423. For the factory default, which is RS-232, the jumper will be between pins 2 and 3 (the bottom 2 pins) of JP8. To select RS-423 mode, the jumper on JP8 should be changed to pins 1 and 2 (the upper pins). For RS-423, the jumper must be installed on JP9. For RS-232, remove the jumper from JP9.

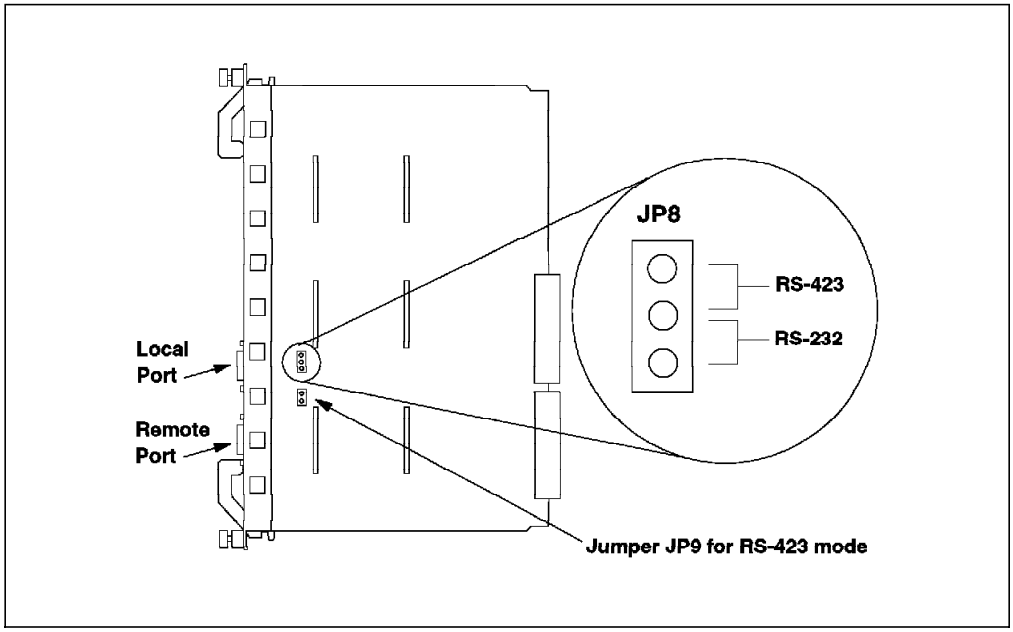


Figure 32. Jumpering for the EC-DMM DB-9 Ports

Holding the DMM by the faceplate, slide it into the slot in the 8260. Like all 8260 modules it can be hot plugged.

If the EC-DMM has been installed correctly and is functioning the status LED should come on. The LCD display should show *diag* then either *rdy* for the master module or *stby* for a backup module.

4.3.2 EC-DMM LED Description

Table 11. EC-DMM Status LED

LED name	Color	State	Indicates
Status	Green	OFF	Power off or module failure
		ON	Power on and software functioning properly
		Blinking	Power on but diagnostics have failed

The LCD display and display control button are used to:

- Display the current operating state of the module.
- Determine the network assignment of ports and 8260 modules in the hub.
- Display the version of the EC-DMM microcode.

The LCD display normally shows the module operating state. Each time the display control button is pressed the character display cycles through each of the networks. By using the network display LEDs on the EC-DMM and the 8260 media modules it is possible to see which modules and which ports are assigned to a network.

For example, we have an 8260 24-port port switching module in slot 2, with ports 1, 3, 5 and 7 assigned to Ethernet_1 and a similar module in slot 4 with ports 15, 16, and 17 assigned to Ethernet_5. If the control button is pressed once the LCD display will change from *rdy* to *E1*. The Ethernet network status LED for Ethernet_1 on the DMM will turn on. The LEDs for ports 1, 3, 5 and 7 on the 8260

Ethernet media module in slot 2 will also turn on to indicate those ports have been assigned to Ethernet_1. If there were more media modules with ports assigned to Ethernet_1 their port LEDs would also turn on. Because Ethernet_2, 3 and 4 are not being used, the next time the button is pressed the LCD display will jump to ″E5″, the DMM network status LED for Ethernet 5 will turn on and the LEDs for ports 15, 16 and 17 on the 8260 Ethernet media module in slot 4 will also turn on to indicate those ports are assigned to Ethernet_5.

To display the EC-DMM microcode version, press the button until the display reads **Vers**. One second after releasing the button the version will be displayed. Table 12 shows the possible states of the display.

Table 12. EC-DMM LCD Display

Display	**Definition**
Diag	The EC-DMM is running diagnostics
Rdy	The EC-DMM is the active (master) management module
Stby	The EC-DMM is in standby mode
Dnld	New microcode is being downloaded
E1-E8,EI	Shows active networks only; EI for isolated
TR1-10,TRI	Shows active networks only; TRI for isolated
F1-F4,FI	Shows active networks only; FI for isolated
Vers	Microcode level of the DMM
LED	Displays when the controller LED test button is pressed

4.4 MAC Daughter Cards

To be able to monitor the network traffic activity on the backplane segments, as well as to be able to communicate with other stations using IP, DMM requires the services provided by MAC daughter cards.

These daughter cards connect to the networks, listen to the traffic flow and pass traffic information back to the DMM. They also provide the DMM with the interface to the networks on the backplane so that it can communicate with the other stations on that network.

The MAC daughter cards are protocol specific cards and at the time of writing this book the following two types of MAC daughter cards were available:

- The E-MAC (Ethernet - Media Access Card)
- The T-MAC (Token-ring - Media Access Card)

These daughter cards can be installed on the media modules that use the same protocol. That is, T-MACs can be installed on token-ring media modules, and E-MACs can be installed on Ethernet media modules. Each token-ring or Ethernet media module can accommodate installation of one MAC daughter card (Ethernet 40-port module allows the installation of two MAC daughter cards). Additionally, the E-MACs can be installed on the EC-DMM. Each EC-DMM can accommodate the installation of up to 6 E-MACs.

Regardless of where the MAC daughter cards are installed, they can be assigned to any of the backplane segments. However, to assign a MAC

daughter card to an isolated segment on a media module, the MAC daughter card must be installed on that media module.

Note

E-MACs installed on EC-DMM can collect detailed statistical information about *all* the ShuntBus and Enhanced TriChannel Ethernet segments. This statistical information includes network as well as module and port level information. This information is collected for both 8260 and 8250 Ethernet modules (note that 8250 Ethernet modules may attach to Ethernet_1 thru Ethernet_3 segments only).

The E-MACs installed on the media modules can collect full statistics (network, module and port level statistics) for Ethernet_4 thru Ethernet_8 segments only. For Ethernet_1 thru Ethernet_3, they can only collect network, module and port level statistics for 8260 Ethernet modules, but for the 8250 modules attached to these segments they can only collect network level statistics and cannot report module or port level statistics. This is due to the use of parallel addressing by the 8250 modules. Therefore, if you are planning to monitor Ethernet_1 thru Ethernet_3 segments which include 8250 Ethernet modules, you must ensure that the E-MACs used to monitor those segments are installed on EC-DMM.

Because of the possibility of installing MAC daughter cards on the 8260 modules, the 8260 modules are identified by *slot* and *subslot* identifiers. Note that the slot and subslot identifiers are used in DMM commands to refer to the media modules, management modules or daughter cards. The following is a summary of how to identify the slot and subslot for each media module, management module, and daughter card:

1. Each media module is always considered to be on the first subslot of the slot on which the media module is installed. For example, if you have installed a 24-port Ethernet media module in slot 2, this will be identified as module 2.1 (slot 2, subslot 1). This is regardless of the fact that the media module may or may not have a MAC daughter card installed on it.
2. If a MAC daughter card is installed on a media module, the daughter card is considered to be in subslot 2 of the slot in which the media module is installed. For example, if the above mentioned 24-port media module had an E-MAC installed on it, the E-MAC will be considered to be module 2.2, whereas the 24-port module is 2.1. Figure 33 is an example of the output if you display all the modules on slot 2.

```
8260A> show module 2.all

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
02.01 1 E24PS-6/8     v1.00   PER_PORT      Port(s) are down
02.02 E-MAC           v2.00   ETHERNET_1

8260A>
```

Figure 33. 24-Port Ethernet Module with E-MAC

3. The stand-alone DMM is always considered to be on the first subslot of the slot in which the stand-alone DMM is installed. Note that a stand-alone DMM does not have the housing for a MAC daughter card.
4. In the case of an EC-DMM which does have the housing for 6 E-MACs, the EC-DMM module is always considered to be in subslot 1 of the slot in which the EC-DMM is installed. Also, the DMM part of EC-DMM is always considered to be in subslot 8. If there are any E-MAC daughter cards installed in the EC-DMM, they will be considered to be in subslots 2 thru 7 of the slot on which EC-DMM is installed. Figure 34 shows how the slot and subslot IDs are used on an EC-DMM.

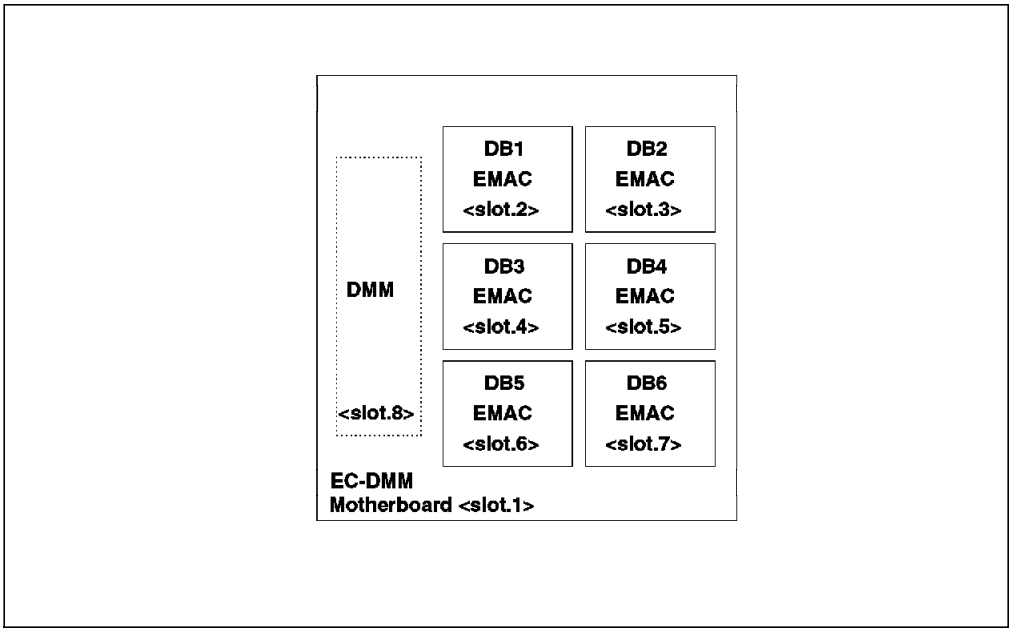


Figure 34. EC-DMM Slots and Subslots

For example, in our 8260, we had an EC-DMM installed in slot 1. This module had an E-MAC installed on the first position (DB1 as shown in Figure 34). If we display this module, the result would be as shown in Figure 35.

```
8260A>
8260A> show module 1.all

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
01.01 1 EC-DMM        v1.00   N/A
01.02 E-MAC           v2.00   ETHERNET_3
01.08 1 DMM           v2.10-H N/A           Master Management Module

8260A>
```

Figure 35. EC-DMM Display

4.4.1 Ethernet MAC Daughter Card (E-MAC)

E-MAC is a MAC daughter card which can be installed on an EC-DMM or Ethernet media modules. Figure 36 shows how you can install up to 6 E-MACs on a single EC-DMM.

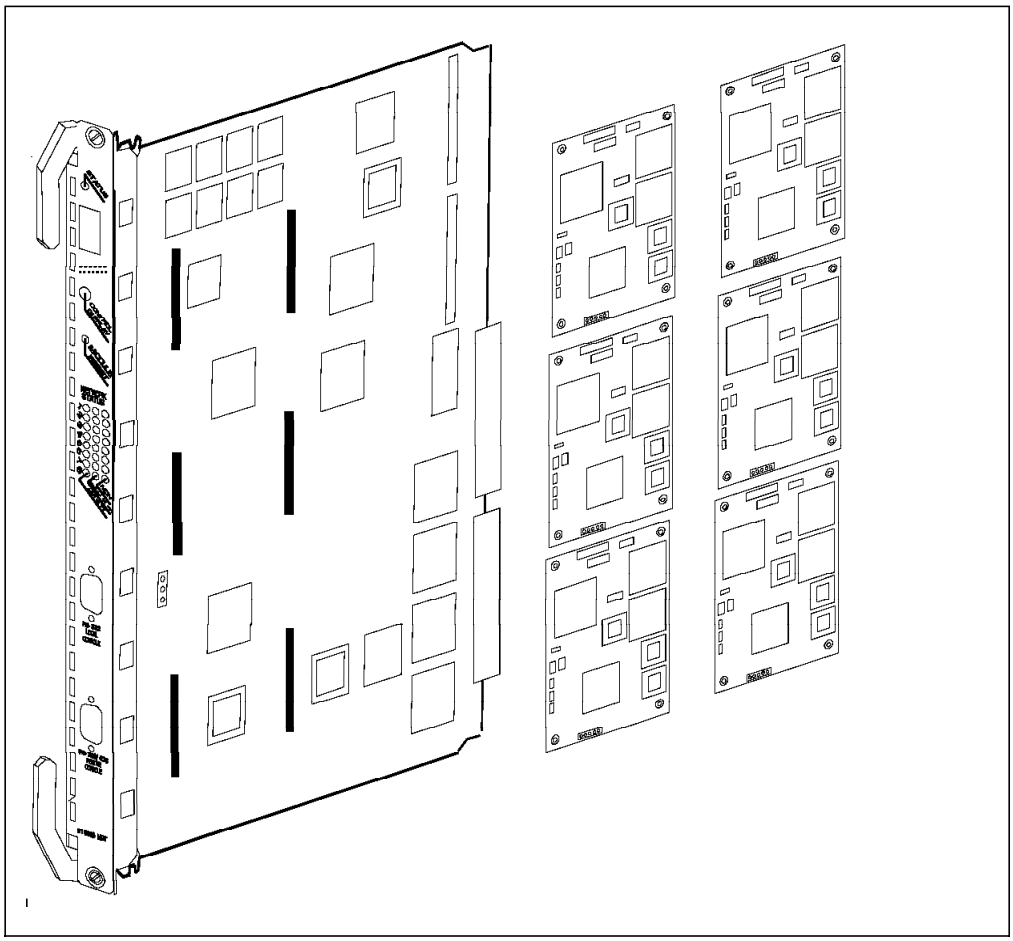


Figure 36. EC-DMM with Up to 6 EMACs

In addition to the DMM with an interface to the network, E-MAC allows you to collect statistics about the Ethernet segment to which it is attached. The statistics which are collected by E-MAC are passed to DMM which allows you to display them locally or access them (in-band) through an application such as RMonitor for AIX. Note that the communication between DMM and the E-MAC installed on the 8260 media modules is via MLAN. For more information about MLAN, please refer to 2.5.1.1, “The Management LAN (MLAN)” on page 26.

The E-MAC supports collection of a subset of the RMON statistics. For information about RMON, and the E-MAC support it, please refer to Chapter 10, “8260 RMON Support” on page 191.

4.4.1.1 Configuration E-MAC

Once you have installed an E-MAC card, you must perform the following configuration steps:

1. Assign IP parameters to the segment to which the E-MAC is going to be attached, as described in 4.2.4.5, “Configuring DMM IP Parameters” on page 54.

2. Use the following command to set an appropriate *mode* for the network interface on the E-MAC:

   ```
   8260A> set module 2.2 interface {enable|disable|standby}
   ```

   The valid *options* for this command are:

   - Enable

     This option allows the network interface on the E-MAC to be activated automatically when attached to a backplane segments. An active E-MAC will be able to send and receive data and collect statistics about the segment to which it is attached. An active E-MAC, when connected to a backplane segment, assumes all the IP parameters assigned to that segment.

   - Disable

     This prevents the network interface on the E-MAC from being activated when attached to a backplane segment.

   - Standby

     This allows the E-MAC to assume the role of backup for the active E-MAC when it is attached to a LAN segment on the backplane. The standby E_MAC will take over from an active E-MAC on that segment, should the active E-MAC fail. When a standby E-MAC takes over the role of the active E-MAC on the segments, it assumes all the IP parameters assigned to the segment. You may use this option when you have two E-MACs attached to the same segment and want one of them to act as a backup for the active E-MAC.

3. Assign the E-MAC to the desired segment using the following example:

   ```
   8260A> set module 2.2 network ethernet_1
   ```

   If you try to assign an E-MAC with *enabled* interface to a segment which already has an active E-MAC, your command will be rejected as shown in Figure 37.

```
8260A> set module 1.2 network ethernet_1


Interface module 2.2 already enabled for this network
Multiple Enabled Interface cards cannot be on the same network
Command aborted

8260A>
```

Figure 37. Assigning E-MAC to a Segment with an Active E-MAC

4. If you are planning to use the RMON support provided by E-MAC, you may perform some additional steps as discussed in 10.6.4, “Collecting and Displaying RMON Groups Using E-MAC” on page 218.

You can use the following example to obtain information about the E-MAC and how it’s configured:

```
8260A> show module 1.2 verbose
```

In this example, the E-MAC is installed in the first subslot of the EC-DMM which is installed in slot 1 of the 8260. The output from this command is shown in Figure 38 on page 66.

```
8260A> show module 2.2 verbose

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
02.02 E-MAC           v2.00   ETHERNET_1

E-MAC: Ethernet Network Monitor Card

Boot Version:                             v1.01
IP Address:                               9.67.46.41
Subnetwork Mask:                          ff.ff.ff.f0
Default Gateway:                          9.67.46.46
Station Address:                          10-00-f1-0c-c0-f7
Interface Mode:                           ENABLED
RMON Host Statistics:                     DISABLED
RMON Probe Mode:                          DISABLED
Interface Number:                         4


8260A>
```

Figure 38. Output from E-MAC Display

Note that this example shows that the E-MAC has a MAC address (shown in non-canonical format in our display because of the DMM setting). This display also shows the IP address, subnet mask, and default gateway for E-MAC which is that of the Ethernet segment to which this E-MAC is assigned.

4.4.2 Token-Ring MAC Daughter Card (T-MAC)

The T-MAC must be mounted on an 8260 token-ring media module. This is because at this stage there is no token carrier DMM. The T-MAC performs the same functions for token-ring as the E-MAC does for Ethernet. It gathers network and port statistics and transmits them to the DMM via the MLAN.

Each token-ring media module has the housing to install one T-MAC.

In addition to providing DMM with the interface to the backplane segments, T-MAC allows you to collect statistics about the token-ring segment to which it is attached. The statistics which are collected by T-MAC are passed to DMM (over MLAN) which allows you to access them locally or in-band through an application such as RMonitor for AIX. T-MAC supports collection of a subset of RMON statistics. For information about RMON, and the T-MAC support for it, please refer to Chapter 10, “8260 RMON Support” on page 191.

4.4.2.1 Configuring T-MAC

Once you have installed the T-MAC card, you must perform the following configuration steps:

1. Assign IP parameters to the segment to which the T-MAC is going to be attached, as described in 4.2.4.5, “Configuring DMM IP Parameters” on page 54.

2. If you are planning to use LAAs within your network, use the following example to assign a locally administered address to T-MAC:

   ```
   8260A> set module 6.2 locally_administered_address 40-00-00-82-60-a1
   ```

   Note that assigning a locally administered address to T-MAC, does not result in the T-MAC using the assigned address automatically. You must use the following command to choose which type of MAC address (locally administered or universal) is to be used by the T-MAC:

   ```
   8260A> set module 6.2 mac_address_type burned_in
   or
   8260A> set module 6.2 mac_address_type locally_administered
   ```

3. Use the following example to enable or disable early token release support of the T-MAC

   ```
   8260A> set module 6.2 early_token_release {enable | disable}
   ```

4. Specify if the T-MAC is going to contend to become the active monitor, using the following example:

   ```
   8260A> set module 6.2 monitor_contention {enable | disable}
   ```

   This parameter affects the way in which the T-MAC participates in the token claiming process as follows:

   - If you enable monitor contention, the T-MAC will always try to contend to become an active monitor.
   - If the monitor contention is disabled and another station on the ring detects the absence of an active monitor and initiates the token claiming process, the T-MAC will not contend to become an active monitor.
   - If the T-MAC is the first station which detects the absence of an active monitor, it will contend to become the active monitor, regardless of the setting of the monitor contention parameter.

5. Use the following example command to set an appropriate *mode* for the network interface on the T-MAC:

   ```
   8260A> set module 6.2 interface {enable|disable|standby}
   ```

   The valid *options* for this command are:

   - Enable

     This option allows the network interface on the T-MAC to be activated automatically when attached to a backplane segment. An active T-MAC will be able to send and receive data and collect statistics about the segment to which it is attached. An active T-MAC, when connected to a backplane segment, assumes all the IP parameters assigned to that segment.

   - Disable

     This prevents the network interface on the T-MAC from being activated when attached to a backplane segment.

   - Standby

     This allows the T-MAC to assume the role of backup for the active T-MAC when it is attached to a LAN segment on the backplane. The standby T-MAC will take over from an active T-MAC on that segment, should the active T-MAC fail. When a standby T-MAC takes over the role of the active T-MAC on the segment, it assumes all the IP parameters assigned to that segment. You may use this option when you have two

T-MACs attached to the same segment and want one of them to act as a backup for the active T-MAC.

6. Assign the T-MAC to the desired segment using the following example:

   ```
   8260A> set module 6.2 network token_ring_10
   ```

   If you try to assign a T-MAC with *enabled* interface to a segment which already has an active T-MAC, your command will be rejected as shown in Figure 39.

```
8260A> set module 8.2 network token_ring_10


Interface module 6.2 already enabled for this network
Multiple Enabled Interface cards cannot be on the same network
Command aborted

8260A>
```

Figure 39. Assigning T-MAC to a Segment with an Active T-MAC

7. If you are planning to use RMON support provided by T-MAC, you may perform the additional steps described in 10.6.6, “Collecting and Displaying RMON Groups Using T-MAC” on page 230.

You can use the following example to obtain information about the T-MAC and how it’s configured:

```
8260A> show module 6.2 verbose
```

In this example, the T-MAC is installed on the 18-port active per-port switching token-ring media module which is installed in slot 6. The output from this command is shown in Figure 40 on page 69.

```
8260A> show module 6.2 verbose

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
06.02 T-MAC           v2.00   TOKEN_RING_10

T-MAC: Token Ring Network Monitor Card

Boot Version:                              v2.00
IP Address:                                9.67.46.235
Subnetwork Mask:                           ff.ff.ff.f0
Default Gateway:                           9.67.46.238
Station Address:                           10-00-f1-0b-09-5f
Locally Administered Address:              40-00-00-82-60-a1
MAC Address Type:                          BURNED-IN
Interface Mode:                            ENABLED
RMON Groups:                               DISABLED
Surrogate Groups:                          DISABLED
Dot5 Group:                                DISABLED
RMON Host Statistics Collection:           DISABLED
RMON MAC Layer Statistics Collection:      DISABLED
RMON Promiscuous Statistics Collection: DISABLED
RMON Ring Station Statistics Collection: DISABLED
RMON Source Routing Statistics Collection: DISABLED
Monitor Contention:                        ENABLED
Adapter Status:                            OPENED
Adapter Microcode Version:                 00 00 01 c1 e3 f1 f7 c3 f1 40
Early Token Release:                       DISABLED
Internal Wrap:                             DISABLED
External Wrap:                             DISABLED
Interface Number:                          5


8260A>
```

Figure 40. Output from T-MAC Display

Note that this example shows that although we have assigned a locally administered MAC address to T-MAC, it is still using the burned-in MAC address. This display also shows the IP address, subnet mask, and default gateway for T-MAC which is that of the token-ring segment to which this T-MAC is assigned.

4.5 Managing 8260 Using DMM and 8250 xMM

This section will explore managing the 8260 hub and its networks using different combinations of 8260 and 8250 management and media modules. There are three possible scenarios for managing an 8260:

1. Managing 8260 with only a DMM
2. Managing 8260 with only 8250 management module(s) and no DMM
3. Managing 8260 with a DMM as well as 8250 management module(s)

Note

The second method is not recommended but will be looked at.

4.5.1 Managing 8260 with DMM

The following is the summary of the capabilities of DMM when managing an 8260 which is populated with both 8260 and 8250 modules:

1. DMM can be used to fully configure the 8260 modules as well as the 8250.
2. DMM in conjunction with E-MAC can be used to monitor the network, module and port-level statistics for the Ethernet segments consisting of 8250 and 8260 modules. However, to be able to monitor the module and port-level statistics for the 8250 modules assigned to Ethernet_1 thru Ethernet_3, the E-MAC must be installed on an EC-DMM.
3. DMM in conjunction with T-MAC can be used to monitor and collect network, module and port-level statistics about the 8260 modules assigned to the token-ring segments on the ShuntBus.
4. DMM and T-MAC cannot be used to monitor token-ring segments on the Enhanced TriChannel. To collect statistics about a token-ring segment on the Enhanced TriChannel, you must use an 8250 TRMM assigned to that segment. If multiple token-ring segments on the Enhanced TriChannel need to be monitored simultaneously, you need one TRMM for each network.
5. DMM cannot be used to monitor FDDI segments on the Enhanced TriChannel. To collect statistics for an FDDI segment on the Enhanced TriChannel, you must use an 8250 FMM assigned to that segment. If multiple FDDI segments on the Enhanced TriChannel need to be monitored simultaneously, you need one FMM for each network.

4.5.2 Managing 8260 with 8250 xMM

The following is a summary of the capabilities of an 8250 xMM when acting as the master management module in an 8260 which is populated with both 8260 and 8250 modules:

1. Each 8250 xMM requires its own payload slot.
2. The 8250 xMM can be used to configure and manage the 8250 media modules installed in the 8260.
3. The 8250 xMM does not recognize and cannot configure the 8260 modules. However, if you use the ″show concentrator″ command, it will report that the slots occupied by the 8260 modules are populated by *ONcore* modules.
4. The 8250 xMM assumes the active controller module occupies slot 17. Because of this slot 17 cannot be used for a media module or a management module and should be used for the right-hand boundary plate of the 8250 mounting kit.
5. Most of the functionality of the 8260 power and cooling subsystems is lost when the 8260 is managed by an 8250 xMM. In this case, the controller module is still able to manage the power and cooling subsystems but there is no interface to enable you to set the parameters for it to perform these functions as you desire. For example, it is not possible to set power classes or set power fault tolerant mode.
6. The backup controller module (if installed) is not recognized and reported by the xMM; however, if it becomes the active controller module, it will be recognized and will be reported to be in slot 17.
7. Any segments on the Enhanced TriChannel (excluding Ethernet_4 thru Ethernet_6) can be monitored using an appropriate xMM attached to that

segment. If multiple 8250 networks need to be monitored simultaneously then each network requires its own 8250 xMM.

8. The two previous points mean that the more monitoring required on 8250 networks the fewer payload slots are available for media modules.
9. ShuntBus based segments are not manageable by 8250 xMM.

4.6 Overview of Management and Control Commands

Commands used in the 8260 hub can be organized into hierarchical or layer like structures. When you first log in to the 8260 hub with the *system* user ID, commands in the first layer will be available. Commands may have various parameters or options associated with them. For example, in Figure 41, all commands in the second layer are the available options associated with the *set* command. Default_gateway, ip_address and subnet_mask are the possible options associated with the *ip* option and the *set* command in the second and first layers in respectively.

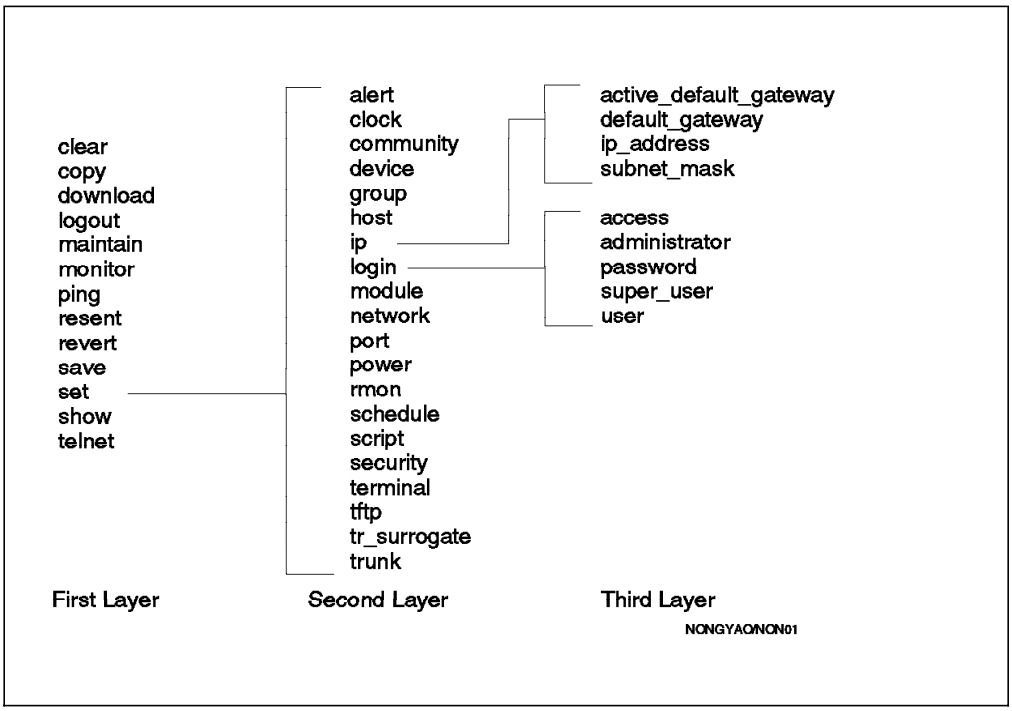


Figure 41. A Sample of Hierarchical Structure Command

In the remainder of this book, the DMM commands will be covered as we discuss various components of the 8260.

Chapter 5. 8260 Intelligent Power Management Subsystem

The 8260 provides extensive power management functions that allow you to take advantage of the modular load-sharing power supply system available on the 8260.

This chapter provides detailed information about the power management subsystem of the 8260.

5.1 Intelligent Power Management Subsystem

The 8260 comes standard with one load-sharing power supply but it allows you to have up to a maximum of four power supplies installed in a single 8260.

Each power supply is hot swappable and is accessible from the front panel of the 8260 hub as shown in Figure 42 on page 74.

The power consumed by the Controller, media and management modules currently installed in the 8260 is evenly distributed over all the installed power supplies. With the 8260 intelligent power management function, which is available thru the Distributed Management Module and the Controller module, you can perform the following functions:

- Assign power class (priority) to each 8260 module.
- Display the power class assigned to each installed module.
- Power up and power down individual slots housing 8260 modules using DMM commands.
- Display the number and status of power supplies installed in the 8260.
- Display the available power budget in your 8260.
- Operate the 8260 in fault-tolerant or non-fault-tolerant mode.
- Display the operational mode (fault-tolerant or non-fault-tolerant) of your 8260.
- Automatically power-down the lower class (priority) 8260 modules if the failure of one or more power supply results in the power requirement of the currently installed modules to exceed the power capacity of the currently operational power supplies.
- Ensure that the newly installed 8260 modules will be powered up only if there is enough available power in the 8260 to operate them.

The following sections are intended to provide detailed information about the various aspects of the intelligent power management in the 8260.

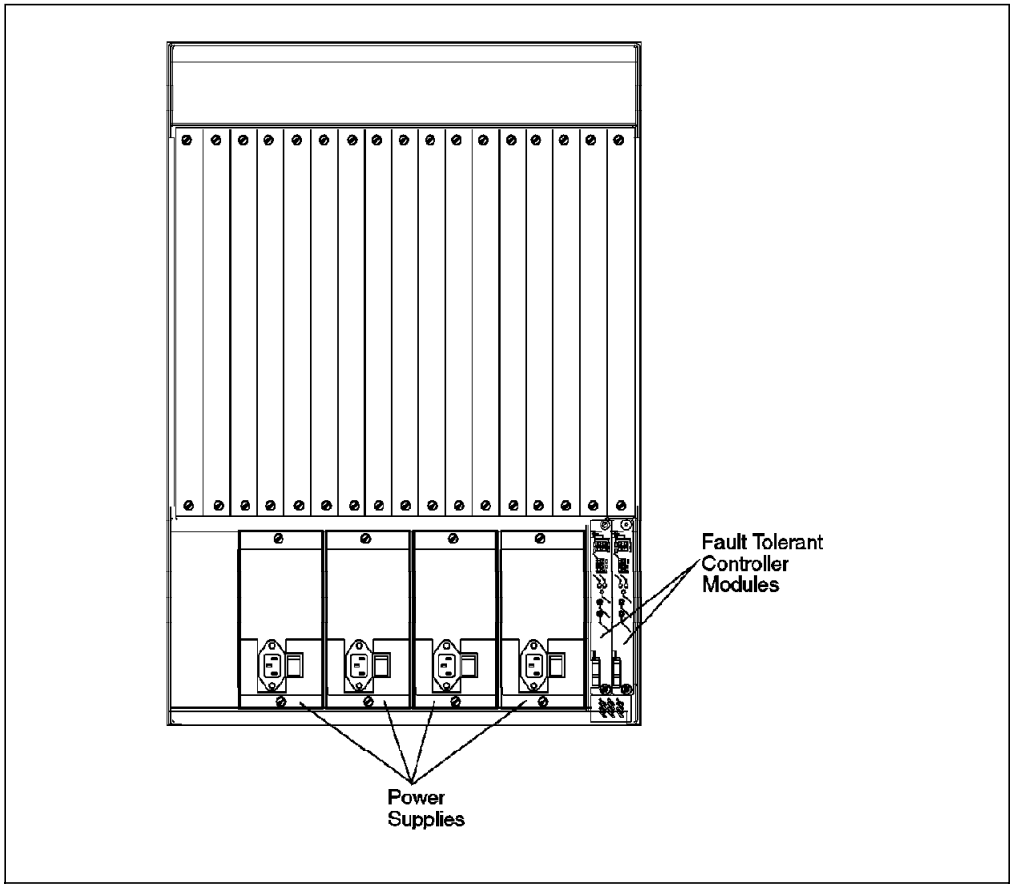


Figure 42. 8260 with 4 Power Supplies

5.2 Power Class

Power class can be considered as a power priority which ranges from 1 to 10. 10 is the highest priority and 1 is the lowest priority.

You may may set the power class for each 8260 module using the following management module command:

```
SET POWER SLOT {slot} CLASS {1 to 10}
```

In the event of failure of one or more power supplies which results in power deficit (that is, the available power is less than the power requirements by all the currently installed modules) the Controller module will power down a number of 8260 media modules with the lowest power class to bring down the level of power consumption to the level of available power supplied by the remaining operational power supply components.

When several modules have the same power class, the 8260 media modules will be powered down from slot 17 to slot 1.

Note: Modules with power class 10 will not be powered down automatically under any circumstances.

The power class is also used during the hub power-up. When an 8260 is powered up, the Controller module will be powered up first, it will then power up all the media modules with the highest power class (power class 10) starting

with slot 1 to 17. The Controller module will repeat this process for all other power classes in descending order of their priority until either all the modules are powered up or the available power supply is exhausted.

Note: You cannot assign a power class to the 8250 modules and they do not take part in the power management. This means that the Controller module cannot exert any control over the 8250 modules as far as the power management is concerned. Therefore, during a power failure, the 8250 modules cannot be powered down by the Controller module and during the hub power up, the 8250 modules will all be powered up regardless of the availability of the power. In this respect, the 8250 modules operate in a manner similar to the 8260 modules which are assigned power class 10.

If you try to assign a power class to an 8250 module, the command will be aborted. An example of this is shown in Figure 43.

```
8260> set power slot 10

Module in slot 10 is not supported.
```

Figure 43. Set Power Class Command for 8250 Modules

Figure 44 shows the use of power classes during power up and power down.

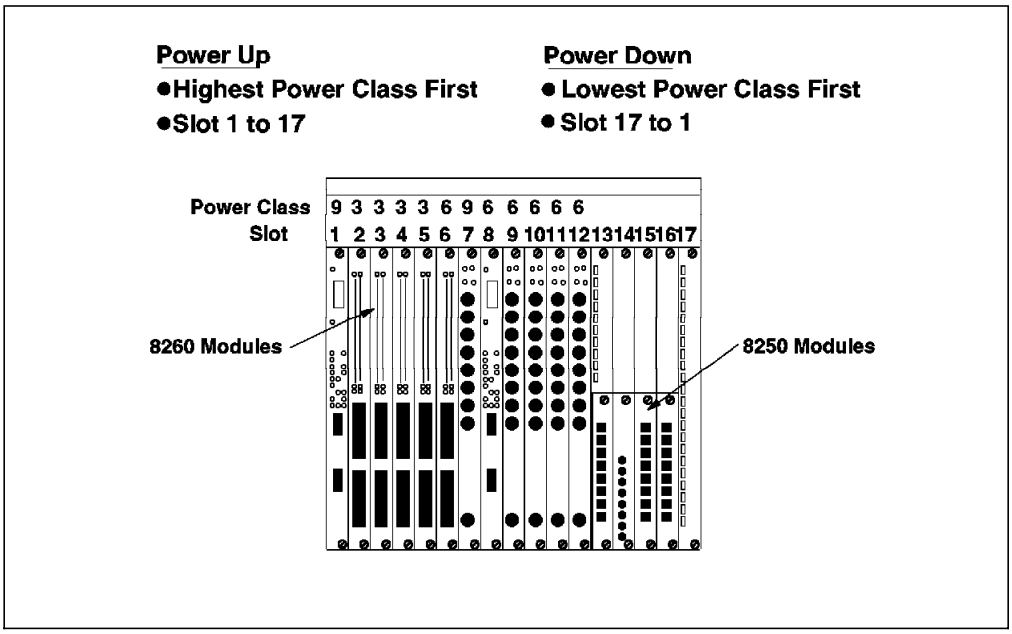


Figure 44. Priorities of Modules to Be Powered-Up or Powered-Down

You can display the power class assigned to individual modules or all the installed modules in the 8260 using the following DMM command:

```
SHOW POWER SLOT {slot|all}
```

An example of the output for this command is shown in Figure 45 on page 76.

```
8260> show power slot all

                Power Management Information
                ----------------------------

Slot Power Information:

Slot     Class          Admin Status        Operating Status
----     -----          ------------        ----------------
1        10             ENABLE              ENABLED
2        3              ENABLE              ENABLED
3        3              ENABLE              ENABLED
5        3              ENABLE              ENABLED
6        9              ENABLE              ENABLED
7        3              ENABLE              ENABLED
8        N/A            ENABLE              ENABLED
9        N/A            ENABLE              ENABLED
10       N/A            ENABLE              ENABLED
11       N/A            ENABLE              ENABLED
12       N/A            ENABLE              ENABLED
13       N/A            ENABLE              ENABLED
14       N/A            ENABLE              ENABLED
15       N/A            ENABLE              ENABLED
16       N/A            ENABLE              ENABLED

8260>
```

Figure 45. Output from Show Power Class Command

Note that in this example, slots 8 thru 16 contain 8250 modules.

Power class is also used by the Controller module to power down media modules in the case of overheating conditions that may be caused by fan failures. This is discussed in Chapter 6, “8260 Intelligent Cooling Subsystem” on page 91.

5.3 Configuring 8260 Power Supplies

The 8260 power management subsystem allows you to install up to a maximum of four power supplies in an individual 8260. The power supplies are hot pluggable and may be installed or removed while the hub is operating.

You can use the following management command to determine the number and status of power supplies installed in your hub:

```
SHOW HUB
```

An example of the output from this command is shown in Figure 46 on page 77.

```
Hub Information:

Hub Type: 58G5801

Backplane Information:

     Backplane Type                                          Revision
     --------------                                          --------
     Load-Sharing Power Distribution Board                    0
     Enhanced TriChannel Backplane                            0
     Ring Backplane                                           0

Power Supply Information:

     Power Supply   Status              Model Number
     ------------   ------              ------------
      1             OKAY                6000PS
      2             OKAY                6000PS
      3             OKAY                6000PS
      4             REMOVED



Temperature Information:

     Probe          Location            Temperature
     -----          --------            -----------
      1             FAN_1               27 Degrees Celsius
      2             FAN_2               29 Degrees Celsius
      3             FAN_3               27 Degrees Celsius

Fan Information:

     Fan            Status
     ---            ------
      1             OKAY
      2             OKAY
      3             OKAY

8260>
```

Figure 46. Output from Show Hub Command

You can use the following management command to determine the amount of power installed and the amount of power budget available in your hub:

```
SHOW POWER BUDGET
```

An example of the output from this command is shown in Figure 47 on page 78.

```
8260> show power budget

                Power Management Information
                ----------------------------

Hub Power Budget :

Voltage Type  Voltage Level  Watts Capacity   Watts Available   Watts Consumed
------------  -------------  --------------   ---------------   --------
    +5V           5.196          551.00          287.00          264.00

    -5V          -5.056           38.25           34.00            4.25

   +12V          12.122          122.50           77.00           45.50

   -12V         -12.150           46.00           42.75            3.25

    +2V           2.140           21.40           17.30            4.10

8260>
```

Figure 47. Output from Show Power Budget Command

The 8260 allows you to set two different power modes, *fault tolerant and non-fault tolerant*.

5.3.1 Non-Fault Tolerant Mode

In the *non-fault tolerant* mode, 100% of installed power supplies will be available to be used by the installed modules. The amount of power available to modules is determined by the number of the installed power supplies as shown in Table 13.

Table 13. Power Available to Modules in Non-Fault Tolerant Mode

Output Voltage	One Power Supply	Two Power Supplies	Three Power Supplies	Four Power Supplies
+5.2 V	204.00 W	367.00 W	551.00 W	735.00 W
+12.0 V	48.00 W	81.50 W	122.50 W	163.00 W
+2.1 V	8.40 W	14.30 W	21.40 W	28.60 W
-5.0 V	15.00 W	27.00 W	38.25 W	51.00 W
-12.0 V	18.00 W	30.50 W	46.00 W	61.25 W
Total	293.40 W	520.30 W	779.15 W	1038.85 W

If a power supply should fail while the hub is operating in non-fault-tolerant mode and the remaining power is not enough to supply all the installed modules, the Controller module will power down 8260 modules according to their power class as described in 5.2, “Power Class” on page 74. This is an attempt to bring the power consumption under the new reduced power budget and also to ensure that the modules with the highest power class will be able to operate normally, using the available power supply. Therefore, it is recommended that you connect the critical components of your networks such as servers, routers, etc. to the 8260 modules with the highest power class.

Note: If a power supply fails and there is still enough power in the hub to operate all the installed modules, the modules will continue their operation without any interruption.

You can configure your 8260 to operate in non-fault-tolerant mode using the following DMM command:

```
SET POWER MODE non_fault_tolerant
```

The current power mode setting for your 8260 can be displayed using the following DMM command:

```
SHOW POWER MODE
```

An example of the output for this command is shown in Figure 48.

```
8260> show power mode

                Power Management Information
                ----------------------------

Hub Power Modes:

        Fault-Tolerant Mode:       NON_FAULT_TOLERANT
        Fault-Tolerant Status:     NON_FAULT_TOLERANT
        Overheat Power Down Mode:  ENABLE

8260>
```

Figure 48. Output from Show Power Mode Command

5.3.2 Fault Tolerant Mode

Installing one power supply more than the required number of power supplies to power all the installed modules will allow you to set the power mode to fault-tolerant. In the *fault tolerant* mode, one power supply's worth of power is kept in reserve. The reserved power is not available to any currently installed or yet-to-be installed modules. It will only be made available to be used by the modules if at least one power supply fails or until you switch the hub from the fault-tolerant mode to non-fault-tolerant mode. In other words, in the fault-tolerant mode the power required by the current and yet-to-be installed modules cannot be greater than the number of installed power supplies minus one (N-1).

The amount of power available to the modules when the hub is operating in fault-tolerant mode is determined by the number of installed modules as shown in Table 14.

Table 14 (Page 1 of 2). Power Available to Modules in Fault Tolerant Mode

Output Voltage	One Power Supply	Two Power Supplies	Three Power Supplies	Four Power Supplies
+5.2 V	N/A	204.00 W	367.00 W	551.00 W
+12.0 V	N/A	48.50 W	81.50 W	122.50 W
+2.1 V	N/A	8.40 W	14.30 W	21.40 W
-5.0 V	N/A	15.00 W	27.00 W	38.25 W

Table 14 (Page 2 of 2). Power Available to Modules in Fault Tolerant Mode				
Output Voltage	**One Power Supply**	**Two Power Supplies**	**Three Power Supplies**	**Four Power Supplies**
-12.0 V	N/A	18.00 W	30.50 W	46.00 W
Totals	N/A	293.40 W	520.30 W	779.15 W

In fault-tolerant mode the 8260 does not reserve any specific power supply in reserve; instead, the reserved power is reserved across all the installed power supplies as shown in Figure 49. This ensures that the failure of any one power supply has no impact on the operation of the hub and the installed modules.

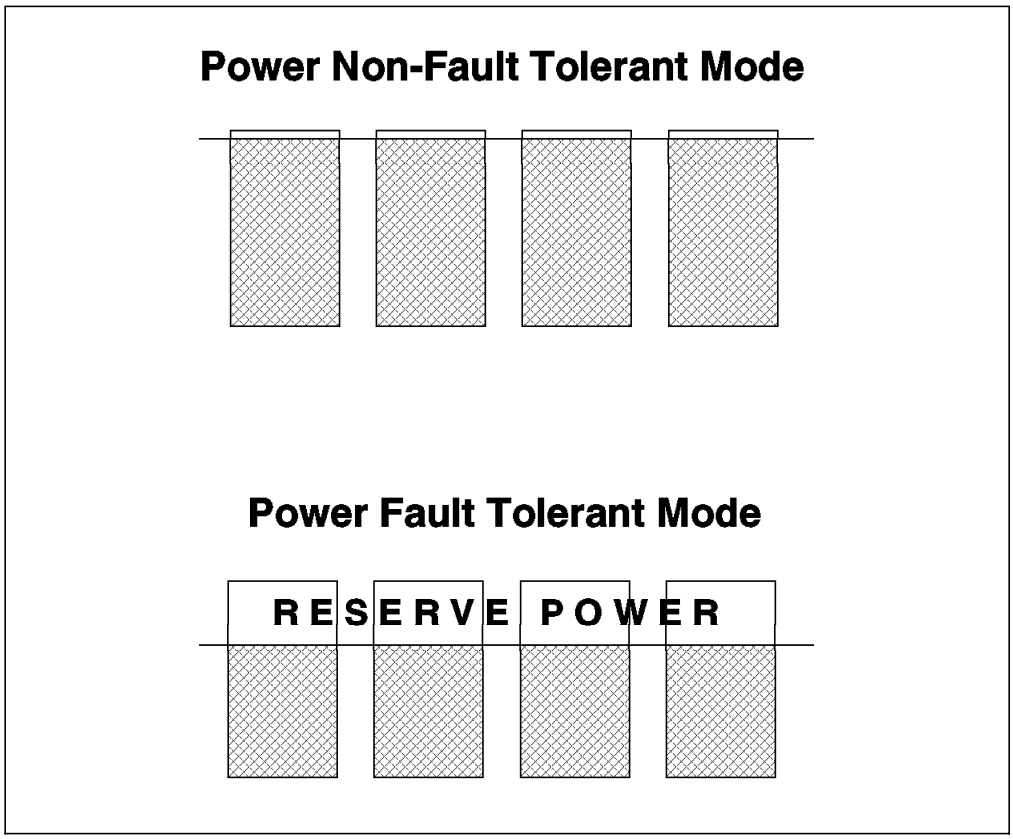


Figure 49. Load Sharing Power Supplies

If a power supply should fail, the power mode will be changed to non-fault-tolerant and the system will supply the reserved power to the installed modules, so that network operations can continue without interruption. Upon the recovery of the failed power supply (for example, by replacing the failed power supply when the 8260 is operating from the other installed power supplies) the 8260 power mode will be changed *automatically* back to the fault-tolerant mode.

You can set your hub to operate in fault-tolerant mode using the following DMM command:

```
SET POWER MODE fault_tolerant
```

5.4 Managing Power in the 8260

The 8260 fault-tolerant Controller module provides extensive power management functions for the 8260 and all its installed modules. However, the capabilities of the Controller module are enhanced via the power management facilities offered by DMM. The following sections examine the impact of DMM on managing the 8260.

5.4.1 Installing 8260 Module in an 8260 Managed by DMM

When a new 8260 module is inserted in the hub which is managed by a DMM, the following functions will be performed:

1. Minimal power is applied to the 8260 module automatically.
2. The 8260 module will use this minimal power to access its EEPROM which contains the Vital Product Data (VPD) about the module. The VPD contains the following information:
   - Module's name and serial number
   - Hardware and software version
   - Manufacturer's ID
   - Date of manufacturing the module
   - Module's power requirements
3. The 8260 module sends its VPD to the Controller module.
4. Controller sends this VPD to DMM. This will allow you to display the Vital Product Data information about all the modules installed in your 8260, using the following DMM command:

   ```
   SHOW INVENTORY
   ```

   An example of the output from this command is shown in Figure 50 on page 82.
5. Controller modules checks the available power budget to see if there is enough power available in the hub to power up the module:
   - If there is enough power, full power will be applied to the 8260 module. The Controller module will then update its power budget to reflect the power consumption by the newly installed module. The new power budget can now be displayed using a DMM command.
   - If there is not enough power to power up the newly installed module, the power will be denied to the module. Therefore, the newly installed module cannot be used.

```
8260>
8260> show inventory

HUB/                    Hardware
Slot  Module            Version  Serial #         Vendor           Date
----- ----------------- -------- ---------------- ---------------- ------
HUB   58G5801           A        H8048            ibm              940313

01.01 1 EC-DMM 1.0      B        1067067          IBM              940421

02.01 1 E24PS-6/8       A        1002683          ibm              940302
02.02 E-MAC             D        1066450          IBM              940409

03.01 6706I-E           XB2      XB26             Retix/Chip       042494

05.01 T20MS             B        1291534          IBM              940805

06.01 T18PSA            D        1292638          IBM              940811
06.02 T-MAC             A        1293023          IBM              940808
06.03 T-JIT             A        1070959          IBM              940810

07.01 1 E10PS-FB-ST     D        1295367          IBM              940813

08.01 T02MS-FIB         N/A      N/A              N/A              N/A

09.01 T02PS-BRG-SRT     N/A      N/A              N/A              N/A

10.01 E04MS-FOIRL       N/A      N/A              N/A              N/A

11.01 E32MS-TS-TL       N/A      N/A              N/A              N/A

12.01 E04PS-FIB         N/A      N/A              N/A              N/A

13.01 T01MS-MGT         N/A      N/A              N/A              N/A

14.01 E12MSS-TELCO      N/A      N/A              N/A              N/A

15.01 EE06PS-RTR        N/A      N/A              N/A              N/A

18.01 8000-RCTL         A        1002380          ibm              940302

19.01 8000-RCTL         A        1002421          ibm              940301

8260>
```

Figure 50. Output from Show Inventory Command

Note: The power class of the newly installed module will not play any role in this process. For example, the Controller module will not power down a currently installed module with a lower power class to accommodate the newly installed module. Also, if the hub is operating in fault-tolerant mode, the hub will **not** switch to non-fault-tolerant mode to use the reserved power to accommodate the newly installed module.

The process of applying power to a newly installed 8260 module is shown in Figure 51 on page 83.

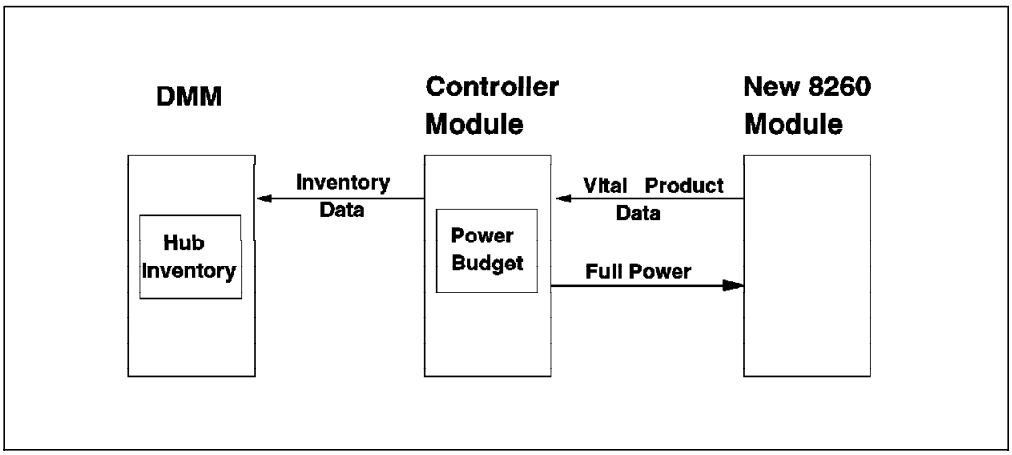


Figure 51. Installing 8260 Modules in an 8260 Managed by DMM

5.4.2 Installing 8260 Module in an 8260 Not Managed by DMM

When a new 8260 module is inserted in the hub and there is no DMM installed in the 8260, the process of powering up the module is identical to what was described above. However, since there is no DMM, you will not be able to display the current power budget despite the fact that the Controller module has accurate information about the current power budget available in the hub.

The process of applying power to a newly installed 8260 module in an 8260 not managed by DMM is shown in Figure 51.

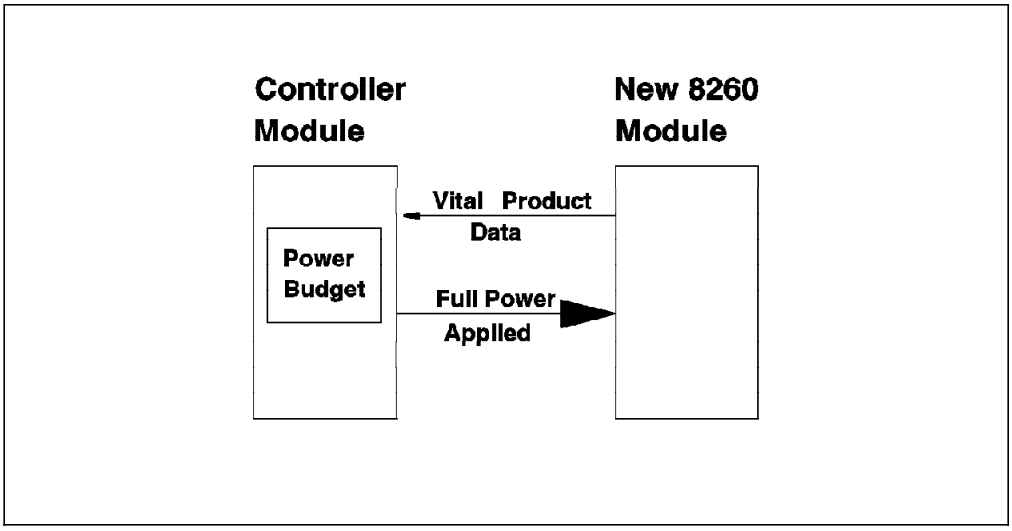


Figure 52. Installing 8260 Modules in an 8260 Not Managed by DMM

5.4.3 Installing 8250 Module in a Hub Managed by DMM

When a new 8250 module is inserted in the hub and the hub is managed by a DMM, the following process will take place:

1. Full power is applied to the module. This is because of the fact that the 8250 modules do not take part in the power management and as soon as they are installed in the hub, they will draw the amount of power that is required for their proper operation.

2. The 8250 module sends *module type* information to the Controller module. The Controller module has no information about how much power is consumed by the module at this stage.
3. The Controller module forwards the *module type* of the newly inserted 8250 module to DMM.
4. DMM has a table which specifies the amount of power required by each 8250 module. This table contains an entry for each *module Type*. DMM retrieves the power requirements of the newly installed module from this table.
5. DMM sends the module's power requirements to the Controller module.
6. Controller module updates its power budget table. At this stage you will be able to display the correct power budget available in the hub using DMM commands.

The process of applying power to a newly installed 8250 module in an 8260 managed hub via DMM is shown in Figure 53.

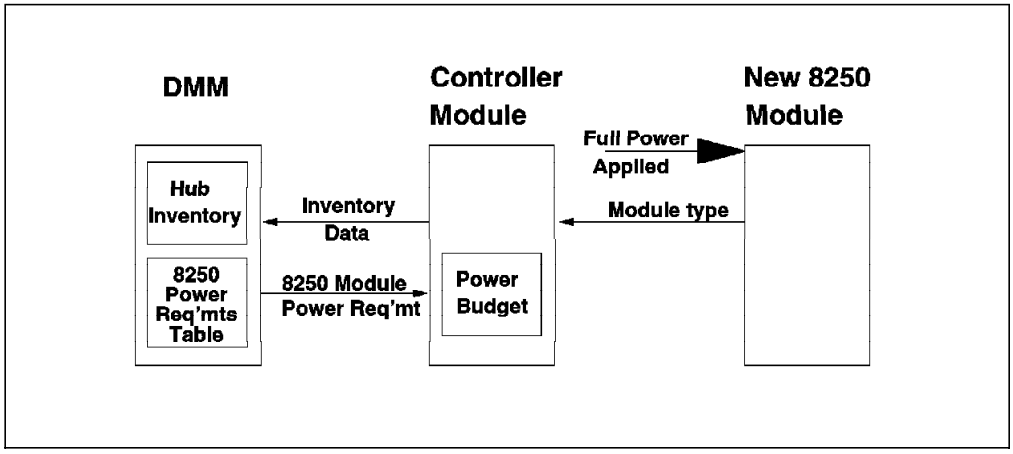


Figure 53. Installing 8250 Modules in an 8260 Managed by DMM

Note: If the power consumption of the newly installed 8250 module results in a power deficit (that is, the total power required by the currently installed modules exceeds the available power supply) the Controller module cannot prevent the power from being used by the newly installed module. Therefore, if you do not check the available power budget in your hub before installing an 8250 module, you may have a situation where the total power consumed by the modules exceeds the available power budget. In this case, the hub may be reset. Following the reset, power will be applied to all the 8250 modules and all the 8260 modules in the order of their power class and slot position as described in 5.2, "Power Class" on page 74. This may result in one or more existing 8260 modules with low power class being denied power after the hub is reset. Therefore, you are strongly advised to ensure that there is enough power available in your hub before you attempt to install a new 8250 module in the 8260. You may refer to the tables provided in Appendix A, "Power Requirements for 8250/8260 Modules" on page 315 to determine the power requirements of the 8250 modules.

5.4.4 Installing 8250 Module in a Hub Not Managed by DMM

When a new 8250 module is inserted in a hub which is not managed by DMM, the process of applying power to the newly installed module is the same as what was described above. However, since there is no DMM, the Controller module is unable to acquire the power requirements of the 8250 module and to update its power budget table. Therefore, installing 8250 modules will result in the Controller module having an inaccurate power budget table which will render the power management of the controller module ineffective. Therefore, you are strongly recommended to ensure that a DMM is installed in the 8260 hub before you attempt to install 8250 modules in the 8260.

The process of applying power to a newly installed 8250 module in an 8260 not managed by DMM is shown in Figure 54.

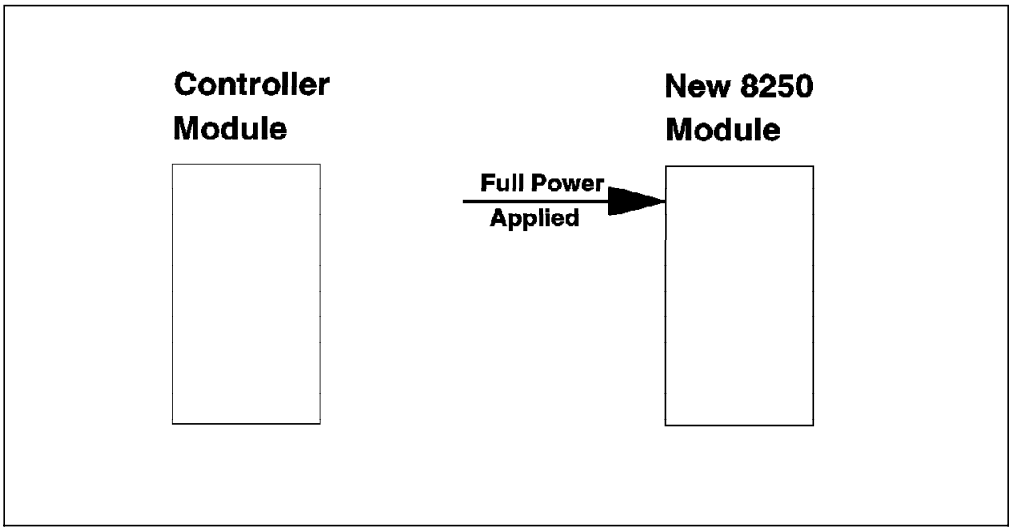


Figure 54. Installing 8250 Modules in an 8260 Not Managed by DMM

5.5 Controlling Power to the 8260 Modules

You can use the following DMM command to enable/disable power to selected slots in your 8260.

```
SET POWER SLOT {slot} MODE {enable|disable}
```

Note that this command is only applicable if an 8260 module is installed in the selected slot. This command does not have any effect on the availability of power to the 8250 modules installed in the selected slot.

Also, note that this command is issued against the slot; therefore, it is not stored in the NVRAM of the 8260 modules installed in that slot.

5.6 Power Management Considerations

- In case of a power failure, the controller might bring down 8260 modules or reset the hub depending on the available power budget and types of modules installed in the 8260.

- When the hub is in the fault-tolerant mode, the reserved power is reserved across all installed power supplies. It is not an individual power supply out of all installed power supplies.
- Although a power class does not apply to the 8250 module, the controller will see the 8250 module having the highest power class, 10.
- Due to a possible power overload situation in a hub that has both 8250 and 8260 modules, it is recommended to install all 8250 modules first and also make sure that the hub has enough power to accommodate the modules.
- To operate the hub in fault-tolerant mode, you must install N power supplies if N-1 can carry the load for the currently installed modules.
- Without DMM in the 8260 hub, the power budget must be calculated manually when you add 8250 module(s) to the hub.

5.7 Power Management Scenarios

Following are three power testing scenarios which were used to simulate a situation where a power failure occurs. We had three installed power supplies in the hub used for testing these scenarios.

- **A Power-Supply Failure - Scenario 1**

  In this scenario, the hub was operating in fault-tolerant mode. In order to simulate a power failure, we turned off one of the power supplies. We then received a message informing us that the system environment had changed and the power supply status had changed to faulty.

```
8260>

Message received from this device on 14:34 Mon 23 May 94:


Enterprise Specific trap:   Environment Change

Message Information:
        Power Supply Status (3):  FAULTY
```

Figure 55. Messages Received when a Power Failure Occurs

- **Show Hub**

  The *show hub* command was used to view the hub environment status and information on power supplies, temperature, and fans. Notice that the 3rd power supply is faulty. In addition, we could see one power supply LED on the active controller module flashing which meant that the corresponding power supply was faulty.

```
8260> show hub

Hub Information:

Hub Type: 58G5801

Power Supply Information:


     Power Supply   Status
     ------------   ------
      1             NORMAL
      2             NORMAL
      3             FAULTY
      4             REMOVED

Temperature Information:

     Probe          Location             Temperature
     -----          --------             -----------
      1             FAN_1           25 Degrees Celsius
      2             FAN_2           25 Degrees Celsius
      3             FAN_3           25 Degrees Celsius

Fan Information:

     Fan            Status
     ---            ------
      1             OKAY
      2             OKAY
      3             OKAY
```

Figure 56. Using the SHOW HUB Command

- **Show Power Mode**

  The *show power mode* command was used to show the current power mode. In this scenario, after taking one power supply down, we still had enough power to support all the installed modules; therefore the hub remained in fault tolerant mode.

```
8260> show power mode

               Power Management Information
               ----------------------------
Hub Power Modes:

        Fault-Tolerant Mode:         FAULT_TOLERANT
        Fault-Tolerant Status:       FAULT_TOLERANT
        Overheat Power Down Mode:    DISABLE
```

Figure 57. Using the SHOW POWER MODE Command

- **A Power Failure - Scenario 2**

  If a power supply should fail and there is not enough power to keep the 8260 in the fault-tolerant mode, you will receive a message informing you that the

system environment is changed and the power status has become non-fault tolerant due to a faulty power supply, as shown below.

```
Message received from this device on 15:47 Mon 23 May 94:


Enterprise Specific trap:   Environment Change

Message Information:
        Power Supply Status (3):  FAULTY



8260>

Message received from this device on 15:47 Mon 23 May 94:


Enterprise Specific trap:   Environment Change

Message Information:
        Hub Power Fault-Tolerant Status :  NON_FAULT_TOLERANT
```

Figure 58. Messages Received when the Power Mode Is Changed

- **Power Mode is Automatically Recovered**

  Upon the recovery of the failed power supply, the power mode will be changed automatically to the fault-tolerant mode.

```
Message received from this device on 15:49 Mon 23 May 94:


Enterprise Specific trap:   Environment Change

Message Information:
        Power Supply Status (3):  ACTIVE



8260>

Message received from this device on 15:49 Mon 23 May 94:


Enterprise Specific trap:   Environment Change

Message Information:
        Hub Power Fault-Tolerant Status :  FAULT_TOLERANT
```

Figure 59. Messages Received upon a Recovery of the Power Supply

- **A Power Failure - Scenario 3**

  In this scenario, we powered down another power supply (in addition to the one powered down in scenario 1). Our hub consists of two 8260 modules (a

DMM and a 24 PPS Ethernet module) and a number of 8250 modules. Both 8260 modules have a power class of 3 assigned to them. Upon taking one power supply down, we found that since the remaining power was not enough to power all the existing modules, the modules with the lowest power priority (the DMM and 24 PPS modules) were powered down by the Controller module.

Note: There will be no message here since the DMM module has been powered-down.

5.8 Installing the 8260 Power Supply

- First, unpack a power supply from the shipping carton and set the ON/OFF switch to OFF.
- Then, remove a blank power supply faceplate in the slot which you will install the power supply.
- Slide the power supply into the selected power supply slot until it is flush with the front of the hub.
- Tighten the 2 spring-loaded screws securely.
- Connect the power cord.
- Turn on the power supply switch.
- Verify power supply operation by checking the active Controller module to ensure that the power supply LED for the installed power supply is okay.

Note:

Replacing or installing a power supply may be done while the hub is running but make sure that you have enough power to support the installed modules.

Chapter 6. 8260 Intelligent Cooling Subsystem

This chapter provides you with information about the 8260 intelligent cooling subsystem.

6.1 Intelligent Cooling Subsystem

The 8260 intelligent cooling subsystem is made up of a number of different components:

- The fans and sensors
- The DMM (Distributed Management Module)
- The Controller module
- The SCI (Serial Control Interface)

All of these components work together to make up the intelligent cooling subsystem.

Each 8260 has three fan units that can be installed or removed while the 8260 hub is operating. These fan units are accessible from the back of the 8260 as shown in Figure 60.

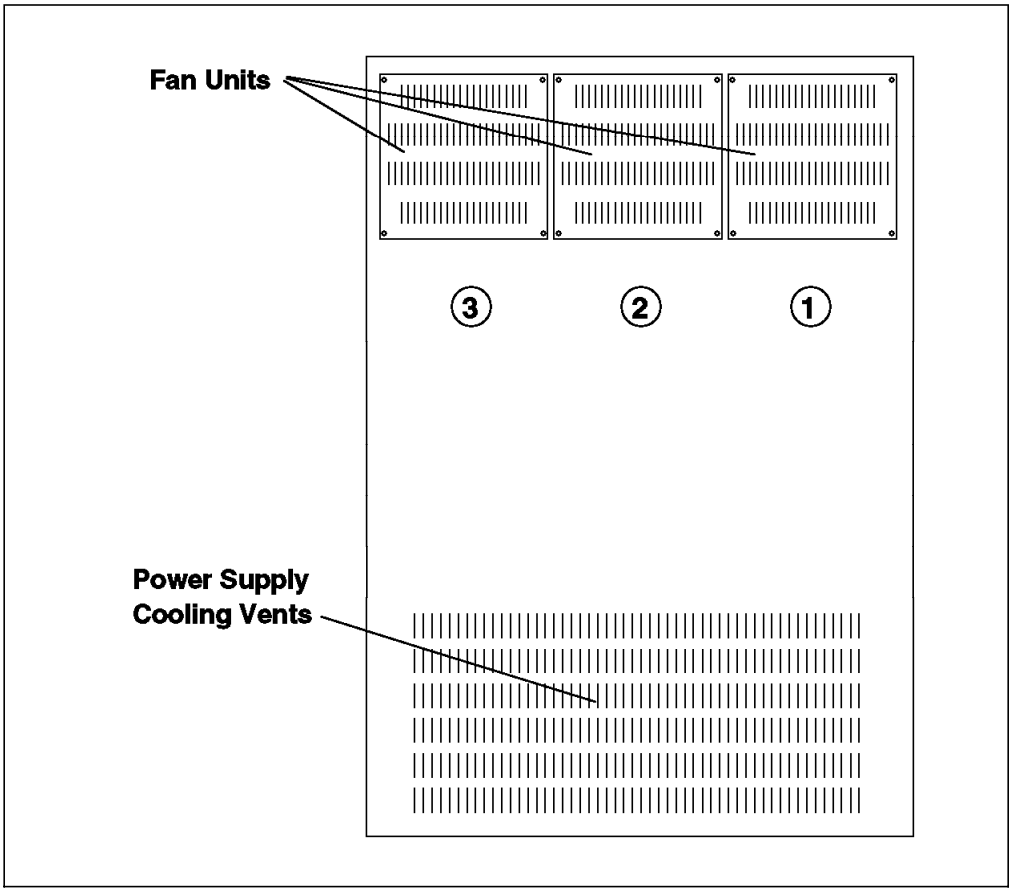


Figure 60. 8260 Fan Units

Each of the three fan units cools an overlapped area in the hub covering 8 slots. The slots covered by each fan unit are:

- Fan 1 - slots 1-8
- Fan 2 - slots 6-13
- Fan 3 - slots 10-17

These 3 areas have their own temperature sensors. Also, integrated into each fan unit is a sensor that detects a stopped or slow fan condition.

The Controller module continually monitors all the sensors via the SCI. You can display the status of the fans and the temperature of the 8260, using the following DMM command:

```
SHOW HUB
```

An example of the output from this command is shown in Figure 61.

```
Hub Information:

Hub Type: 58G5801

Backplane Information:

     Backplane Type                                        Revision
     --------------                                        --------
     Load-Sharing Power Distribution Board                  0
     Enhanced TriChannel Backplane                          0
     Ring Backplane                                         0

Power Supply Information:

     Power Supply   Status               Model Number
     ------------   ------               ------------
      1             OKAY                 6000PS
      2             OKAY                 6000PS
      3             OKAY                 6000PS
      4             REMOVED



Temperature Information:

     Probe          Location             Temperature
     -----          --------             -----------
      1             FAN_1                27 Degrees Celsius
      2             FAN_2                29 Degrees Celsius
      3             FAN_3                27 Degrees Celsius

Fan Information:

     Fan            Status
     ---            ------
      1             OKAY
      2             OKAY
      3             OKAY

8260>
```

Figure 61. Output from Show Hub Command

If a fan unit stops or the temperature in any of the three cooling zones rises above 60 C, the Controller module may, depending on a user configurable parameter (Overheat_Auto_Power_Down) use the SCI bus to power down some of the 8260 modules in the affected cooling zone in order to bring down the temperature to an acceptable level.

The setting of the Overheat_Auto_Power_Down parameter is controlled by the following DMM command:

```
SET OVERHEAT_AUTO_POWER_DOWN {enable|disable}
```

If you set this parameter to *enable*, the controller module will automatically power down some of the 8260 modules in the affected cooling zone in response to an overheat condition. If this parameter is disabled, the controller module will not power down any modules if the temperature rises above 60 in any of the cooling zones.

Note: Disabling the Overheat_Auto_Power_Down may result in damage to the 8260.

You can display the setting of the Overheat_Auto_Power_Down parameter using the following DMM command:

```
SHOW POWER MODE
```

An example of the output from this command is shown in Figure 62.

```
8260> show power mode

                Power Management Information
                ----------------------------

Hub Power Modes:

        Fault-Tolerant Mode:       NON_FAULT_TOLERANT
        Fault-Tolerant Status:     NON_FAULT_TOLERANT
        Overheat Power Down Mode:  ENABLE

8260>
```

Figure 62. Output from Show Power Mode Command

The following section describes the mechanics of the intelligent cooling subsystem:

- Each of the 8260 modules can be assigned a power class. By default, the 8260 modules are shipped from the factory with a power class setting of 3.
- 8250 modules cannot be assigned a power class. By default, they are effectively assigned a power class of 10.
- If an overheat condition is detected there is a one-minute delay and then the DMM is notified.
- DMM will generate an SNMP alert as a result of receiving an over temperature notification. This alert will be displayed on the local console attached to the DMM. The alert is also sent to any SNMP manager which is defined in the community table of the DMM as a *trap receiver*.
- If the Over_Heat Power_Down is set to Enable, (default is Disable) then the power subsystem is used to power down 8260 modules according to their

power class and slot position within the affected cooling zone as shown if Figure 63 on page 94.

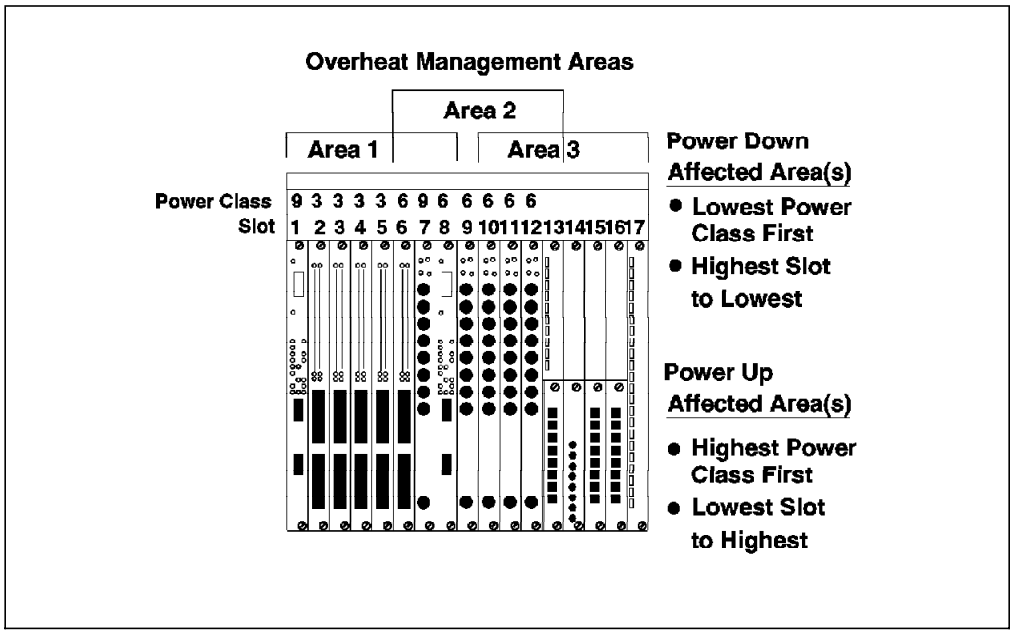


Figure 63. 8260 Cooling Zones and Power Classes

- Modules are powered down until the 5 volt power supply consumption is reduced by 50 watts.
- The temperature is allowed to stabilize for 15 minutes and if the temperature is still too high, all the 8260 modules in the affected zone are powered down.
- When the overheat condition is resolved the modules are powered back up. Modules with the highest priority are powered up first.
- The 8250 modules and the 8260 modules with power class 10 cannot be powered down by the Controller module.
- If the Overheat_Auto_Power_Down is disabled, the Controller module will not take any action. If the over temperature condition continues, the 8260 may be damaged.

The above process is shown in Figure 64 on page 95.

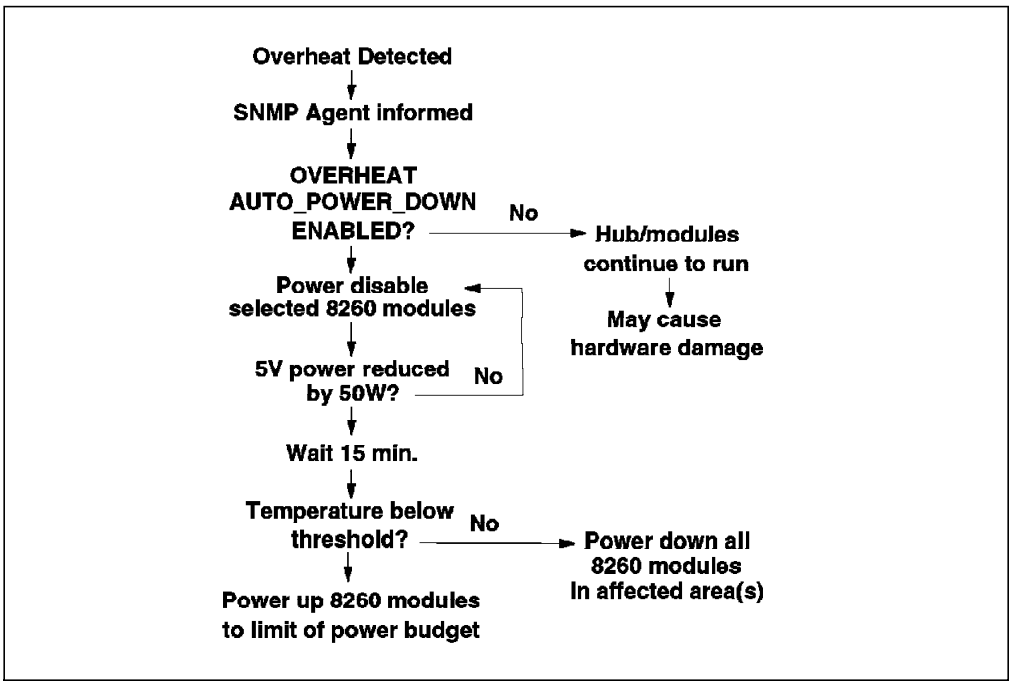


Figure 64. Flow Chart for an Overheat Condition

Chapter 7. 8260 Ethernet Modules

This chapter will describe the Ethernet modules for the 8260 multiprotocol intelligent switching hub. Each module will be described along with its features and the necessary steps required to configure these modules. Where necessary, examples will be given of where the module would be used. Currently, the available 8260 Ethernet modules are:

- 8260 Ethernet 24-Port 10Base-T Module
- 8260 Ethernet 10-Port 10Base-FB Module
- 8260 Ethernet 20-Port 10Base-T Module
- 8260 Ethernet 40-Port 10Base-T Module
- 8260 Ethernet Security Daughter Card

Also, note that you can install and use any 8250 Ethernet module in the 8260 multiprotocol intelligent switching hub. For information about the 8250 Ethernet modules please refer to *IBM 8250 Intelligent Hub and IBM HUB Management Program/6000, (GG24-4033)*.

7.1 Ethernet LAN Overview

The following is a brief introduction to Ethernet. For further information about the Ethernet LAN architecture, please refer to *LAN Concepts and Products, GG24-3178-03*.

Though Ethernet V2 and 802.3 are not identical, the term *Ethernet* is widely used to describe LANs that use either protocol. As most of the information in this book applies equally to both Ethernet V2 and 802.3 LANs, the term Ethernet (802.3) will be used throughout this book. However, where there are differences, they will be indicated by using the appropriate terminology.

The Ethernet architecture uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the protocol to control the Ethernet bus operation. As the name implies, CSMA/CD permits multiple stations to access the Ethernet; however, only one station can occupy the bus at any time.

7.1.1 CSMA/CD

The CSMA/CD protocol is simple and straightforward:

- When a station wants to transmit some data, it has to first listen to ascertain whether the bus is occupied or not.
- If the bus is free, the station starts transmitting immediately.
- If the bus is busy, the station waits and continues to listen until no activity is detected on the bus. It starts to transmit its data only when the bus has been cleared of any traffic.

Occasionally, two stations can begin to transmit simultaneously. This results in a condition known as a *collision*. To resolve this condition, both stations stop transmitting, wait for a random interval, listen again and retransmit when the bus is free. If a station's subsequent attempt results in another collision, its wait time will be doubled and the cycle is repeated. This cycle may be repeated up

to 16 times consecutively, after which the station reports a transmission error to the higher layer protocol. The probability of a collision occurring is directly proportional to the number of stations, frequency of transmissions, size of frames, and length of the LAN segment.

Under the 802.3 specifications, no station can monopolize the network by sending more data than is allowed. Occasionally, a misbehaving application or a faulty adapter may transmit more data than is allowed. This gives rise to a condition called *jabber*. *Jabber* refers to the transmission of a packet whose length is greater than 1518 octets. Where repeaters are used to extend the Ethernet LAN, jabber can also occur when the transceiver that is attached to the repeater has Signal Quality Error (SQE) set to on.

7.1.2 Frame Size

In the Ethernet LAN environment, all data transmission must occur using Ethernet or IEEE 802.3 frame formats. For details on Ethernet and IEEE 802.3 frame formats, please refer to *LAN Concepts and Products, GG24-3178-03.*

IEEE 802.3 and Ethernet specify a minimum frame size (header plus data) of 64 octets while the largest frame is 1518 octets. A packet whose frame size is less than 64 octets is called an *undersized packet* or a *runt* and *oversized packet* refers to a packet whose frame size exceeds 1518 octets.

7.1.3 Data Integrity

To ensure integrity of the data being transmitted, each data frame is appended with Frame Check Sequence (FCS) information. The FCS information is computed by the transmitting station using a cyclic redundancy algorithm executed against the contents of the data frame to be sent. The same algorithm is used by the receiving station to recompute the FCS on the data frame received.

A *Cyclic Redundancy Checksum (CRC) Alignment Error* will be reported by the receiving station when there is a mismatch between the receiver-computed FCS and the sender's FCS.

7.1.4 Ethernet Addressing Mode

In Ethernet, there are three types of addressing modes:

- Direct addressing

  In the direct addressing mode, the sender station has to know the Ethernet address of the receiver station before communication can occur.

- Broadcast

  Broadcast addresses a frame to all stations in the network. It uses a special code in the destination address field. When a broadcast is transmitted, it is received and processed by every station in the network.

- Multicast

  Multicast addresses a frame to a subset of stations in the network. It uses a special *group address* to allow multiple stations to listen to a single address. When a frame is sent to a group address, all stations subscribing to that group will receive it.

7.2 8260 Ethernet 24-Port 10Base-T Module

The 8260 Ethernet 24-Port 10Base-T Module is a 24-port IEEE 802.3 repeater module that complies with the 10Base-T standard and supports backbone and to-the-desk connectivity over Unshielded Twisted Pair (UTP) cabling. This module provides two 50-pin Telco-type connectors. Each Telco-connector can be connected to an external 12-port *harmonica*. Each port on the harmonica provides an RJ-45 connector for attaching 10Base-T compliant devices using UTP cabling for distances of up to 100 m.

Note that all 24-ports are internally crossed-over which allows you to connect them directly to 10Base-T transceivers without using external crossover adapters.

The 8260 Ethernet 24-Port 10Base-T Module can also be used to provide a UTP backbone connection between the 8260 and other 10Base-T compliant hubs such as another 8260, 8250 or 8224. In this case, an external crossover adapter is required.

Note that because of limited achievable distances, the UTP backbone is not recommended. Instead, you are advised to use a fiber (10Base-FL or 10Base-FB) module for backbone connectivity.

The 8260 Ethernet 24-Port 10Base-T Module provides the following features:

- Per-port switching

  Each port can be connected to one of the eight segments on the backplane. Also, the module provides eight isolated segments to which the individual ports on the module can be attached. These isolated segments can be used to set up segments consisting of the users attached to that module without using any backplane resource.

  Note

  The 8260 Ethernet 24-Port 10Base-T Module supports up to 6 segments simultaneously. This means that the ports on this module can be connected to a maximum of 6 segments which can be a combination of backplane and isolated segments.

- Support for 1 E-MAC

  This module provides the mounting for one E-MAC. The E-MAC can be assigned to any of the Ethernet segments on the backplane, or any of the isolated segments on this module. Note that the E-MAC mounted on this module cannot collect per-port or per-module statistics about the 8250 modules.

- Support for 1 Ethernet Security Card

  In addition to mounting for the E-MAC, this module provides the mounting for one Ethernet security card. Ethernet Security card provides for eavesdropping and intrusion control for your Ethernet segments. For information about Ethernet Security Card, please refer to 7.11, “8260 Ethernet Security Daughter Card” on page 121.

- Support for port redundancy

  You can set up redundancy between two links on the same module or two different modules. Note that port redundancy is supported between different

types of modules. For example, you can set a 10Base-T port on an 8260 Ethernet 24-Port 10Base-T Module to be a redundant port for 1 10Base-FB on the 8260 Ethernet 10-Port 10Base-FB Module.

- Auto-polarity detection

  You can enable/disable auto-polarity detection for each port on the module. When enabled, this feature will automatically detect if you have erroneously reversed polarity of the cable during its assembly and will resolve the problem by reversing the polarity.

- Support for non-10Base-T compliant devices

  This module allows you to disable link integrity which allows connection to some equipment that does not conform to the 10Base-T standard.

When designing Ethernet segments consisting of the 8260 Ethernet 24-Port 10Base-T Module, you must use the following *Equivalent Distances* for this module:

Table 15. Equivalent Distances for 24-Port 10Base-T Module

8260 Module	**Equivalent Distance (meters)**
24-port 10Base-T Module	585
Incoming signal to TP port	420
Outgoing signal to TP port	165

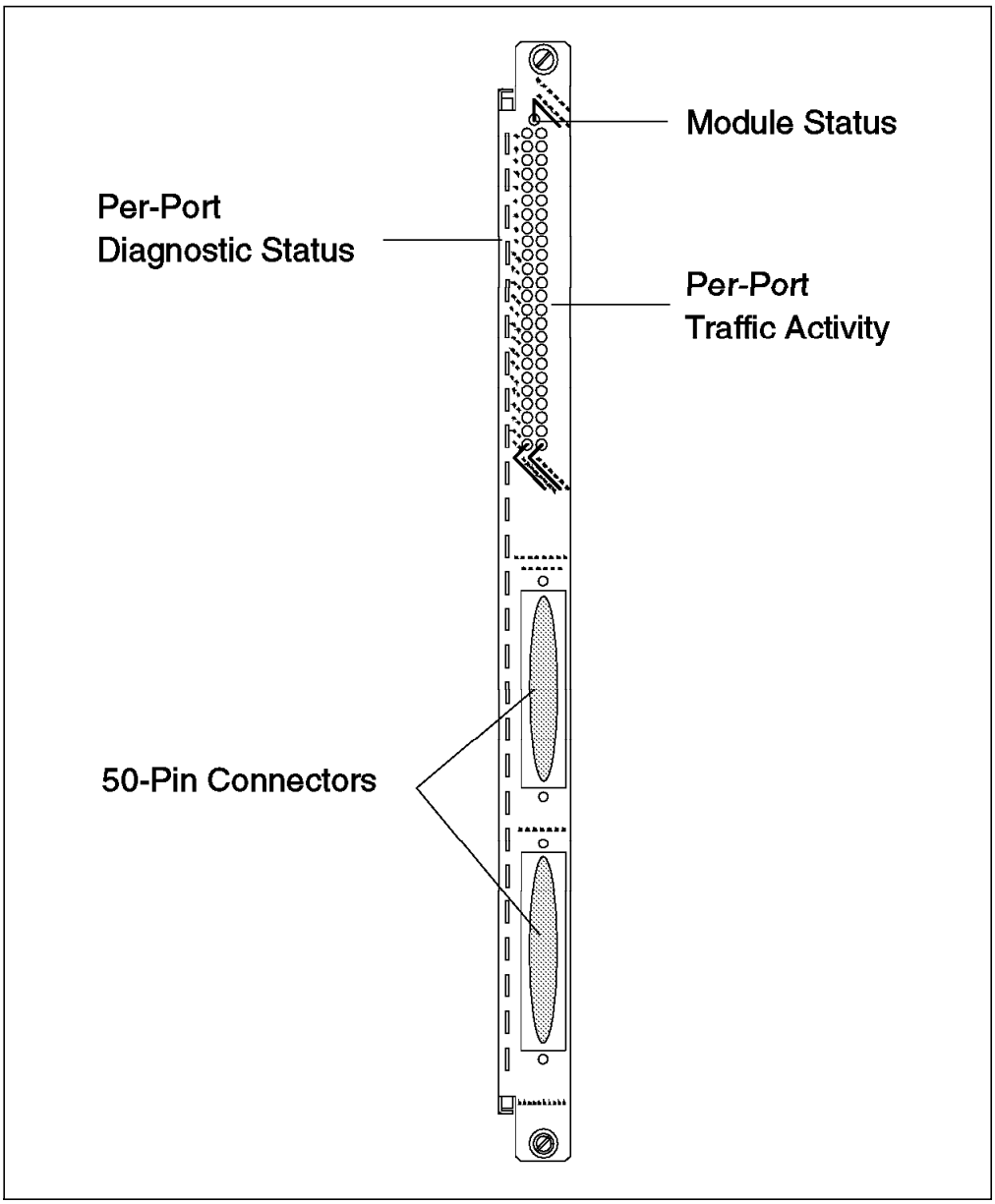


Figure 65. Front View of 24-Port 10Base-T Module

Figure 65 shows the front view of the 8260 Ethernet 24-Port 10Base-T Module. As can be seen, the 8260 Ethernet 24-Port 10Base-T Module provides you with LED Indicators on the front panel that allow you to monitor the status of the module and the individual ports. Table 16 describes the meaning of these LEDs:

Table 16 (Page 1 of 2). 24-Port 10Base-T Module LED Descriptions

LED Name	Color	State	Description
Module Status	Green	On	Module powered up OK
		Off	No Power.
		Blinking	Module failed self diagnostics

Table 16 (Page 2 of 2). 24-Port 10Base-T Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
Activity	Yellow	On	Constant activity on the port
		Off	No packets received on the port
		Blinking	Normal activity on the port
Status	Green	On	Port enabled and link OK
		Off	Port disabled.
		1 Blink	Link failure on the port
		2 Blinks	Port partitioned

Figure 66 shows the side view of the 8260 Ethernet 24-Port 10Base-T Module. As can be seen, in addition to the 8 isolated segments and the mounting for the E-MAC, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored unless DIP_Configuration is enabled for DMM. For more information, please refer to 4.2.4.4, " Configuring DMM Device" on page 50.

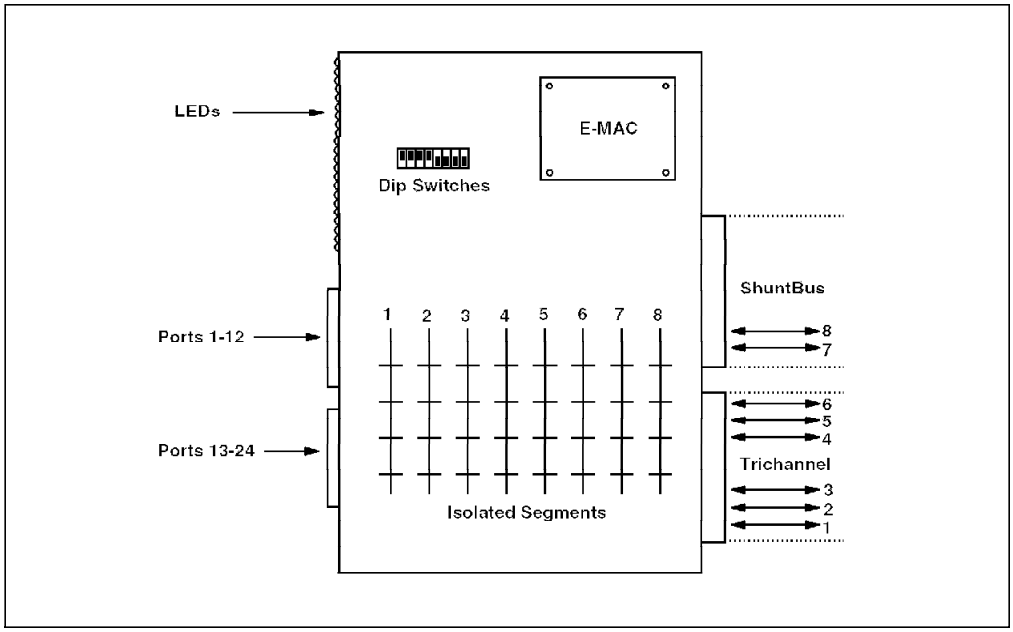


Figure 66. 24-Port 10Base-T Module Side View

The expanded view of the DIP switches is shown in Figure 67 on page 103.

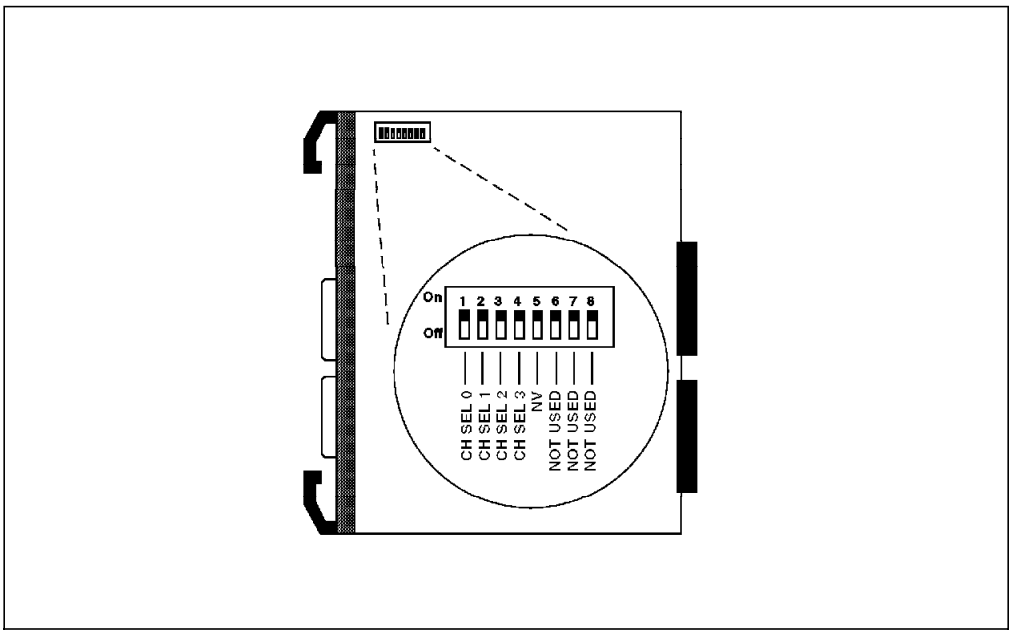


Figure 67. 24-Port 10Base-T DIP Switches

The DIP switches let you perform the following:

- Use DIP switch positions 1 through 4 to assign all the ports on the module to one of the backplane segments or an isolated-1 segment. Note that when using DIP switches, all the ports will be assigned to the same segment, so you cannot do per-port switching when using DIP switches for configuring your the 8260 modules.

  Table 17 shows the meaning of settings for DIP switches 1 thru 4:

Table 17. 24-Port 10Base-T Module DIP Switch Settings

Network Selection	Switch 1	Switch 2	Switch 3	Switch 4
Ethernet_1	OFF	ON	ON	ON
Ethernet_2	ON	OFF	ON	ON
Ethernet_3	OFF	OFF	ON	ON
Ethernet_4	ON	ON	OFF	ON
Ethernet_5	OFF	ON	OFF	ON
Ethernet_6	ON	OFF	OFF	ON
Ethernet_7	OFF	OFF	OFF	ON
Ethernet_8	ON	ON	ON	OFF
Isolated_1	ON	ON	ON	ON

  By default, the module is shipped from the factory with the DIP switches set for Ethernet_1.

- Use DIP switch position 5 to choose if the module is going to use the Non-Volatile RAM (ON position) or DIP switch settings (OFF position) for its configuration. Note that if there is a management module installed in the 8260, this DIP switch determines which configuration (NVRAM or DIP switch setting) will be sent to the management module. The actions taken by the management module, upon receipt of this information are described in

4.2.4.4, “ Configuring DMM Device” on page 50. By default, DIP switch 5 is set to NVRAM.

7.3 10Base-T Module Usage

Figure 68 provides an example of the usage of the 8260 Ethernet 24-Port 10Base-T Module.

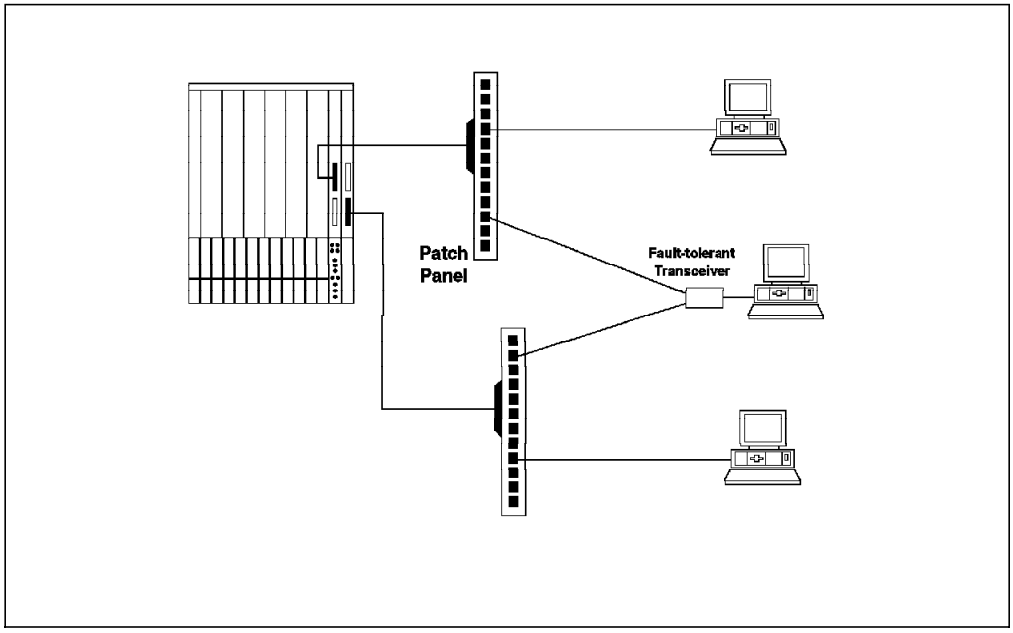


Figure 68. 24-Port 10Base-T Module Usage

7.4 Configuring the 10Base-T Module

To configure the 8260 Ethernet 24-Port 10Base-T Module you must do the following:

- Select network for each port

  Each port can be assigned to one of the 8 Ethernet segments on the backplane or one of the 8 isolated segments on the module. Note that the ports can be connected to a maximum of six backplane and/or isolated segments simultaneously.

  The port assignment can be done via onboard dip switches or the following management module command:

  ```
  SET PORT {slot.port} NETWORK {network}
  ```

  Note

  When using DIP switches on the 8260 Ethernet 24-Port 10Base-T Module, it is only possible to assign all the ports to the same network. This network can be one of the 8 Ethernet segments on the backplane, or isolated_1.

- Enable/disable ports

Each port on the 8260 Ethernet 24-Port 10Base-T Module can be enabled/disabled independently from the other ports. You can use the following management module command to enable/disable a port:

```
SET PORT {slot.port} MODE {enable|disable}
```

- Set port redundancy

  The port redundancy feature allows you set redundancy between two ports. The two ports can be on the same or different modules and can be of the same or different types. For example, a 10Base-T port can be defined to be a redundant port for a 10Base-FB port. Port redundancy is allowed between the 8250 and the 8260 ports. You can use the following management module command to set port redundancy:

  ```
  SET PORT {slot.port} MODE REDUNDANT {slot.port}
  ```

  When port redundancy is no longer required, you can use the following management command to set the port to operate in non-redundant mode:

  ```
  SET PORT {slot.port} MODE NON-REDUNDANT
  ```

- Enable/disable auto-polarity

  This feature enables the 8260 Ethernet 24-Port 10Base-T Module to automatically switch the polarity of the twisted-pair cabling in case the polarity of the cabling has been erroneously reversed during the cable assembly. To enable auto polarity detection and reversal on each port, you can use the following management module command:

  ```
  SET PORT {slot.port} AUTO_POLARITY {enable|disable}
  ```

- Enable/disable link integrity

  To connect older equipment, that does not fully comply with the 10Base-T standard, to this module, you may have use the following management module command to disable the link integrity:

  ```
  SET PORT {slot.port} LINK_INTEGRITY {enable|disable}
  ```

- Enable/disable port alert

  You may use the following command to enable/disable the sending of port up and down alerts from the individual ports on this module:

  ```
  SET PORT {slot.port} ALERT_FILTER {enable|disable}
  ```

  This command may be used to allow you to monitor the status of the crucial ports on your network while the alerts from the other ports are disabled.

- Enable/disable remote diagnostics

  The Remote Diagnostics feature allows this module to detect certain unusual failure conditions when used in conjunction with the IBM Fault-Tolerant 10Base-T Transceivers. You can use the following management command to enable/disable remote diagnostics:

  ```
  SET PORT {slot.port} MODE {remote_diagnostics|non_remote_diagnostics}
  ```

Note

The 10Base-T specification specifies a minimum of 31 collisions prior to partitioning of a port. The 8260 Ethernet 24-Port 10Base-T Module automatically partitions a port when more than 63 collisions are detected on that port. This value cannot be changed by the users.

7.5 8260 Ethernet 20/40-Port 10Base-T Module

The 8260 Ethernet 20-Port 10Base-T Module, a single-slot 20-port, and the 8260 Ethernet 40-Port 10Base-T Module, a two-slot 40-port are IEEE 802.3 repeater modules that comply with the 10Base-T standard and support backbone and to-the-desk connectivity over Unshielded Twisted Pair (UTP) as well as Shielded Twisted Pair (STP) cabling. These modules provide 20 or 40 shielded RJ-45 connectors for attaching 10Base-T compliant devices using STP and/or UTP cabling for distances of up to 100 m.

Note

You can mix UTP and STP cabling on a single 20/40-port 10Base-T module.

On the 20/40-port 10Base-T modules, all the ports are internally crossed-over which allows you to connect them directly to 10Base-T transceivers without using external crossover adapters.

These modules can also be used to provide UTP/STP backbone connections between the 8260 and other 10Base-T compliant hubs such as another 8260, 8250 or 8224. In this case, an external cross-over adapter is required. As the STP cabling is not part of the 10Base-T specification, when using STP cabling, you must ensure that the hub at the other end is also capable of supporting STP cabling.

The 24/40-port 10Base-T modules provide the following features:

- Per-port switching

  Each port can be connected to one of the eight segments on the backplane. Also, the module provides eight isolated segments to which the individual ports on the module can be attached. These isolated segments can be used to set up segments consisting of the users attached to that module without using any backplane resource.

  Note

  The 20/40-port 10Base-T modules support up to 8 segments simultaneously. This means that the ports on these modules can be connected to a maximum of 8 segments which can be a combination of backplane and isolated segments.

- Support for 2 E-MACs

  These modules provide the mounting for two E-MACs. An E-MAC can be assigned to any of the Ethernet segments on the backplane, or any of the isolated segments on the module. Note that the E-MAC mounted on these modules cannot collect per-port or per-module statistics about the 8250 modules.

- Support for 1 Ethernet security card

  In addition to mounting for two E-MACs, these modules provide the mounting for one Ethernet security card. The Ethernet security card provides for eavesdropping and intrusion control for your Ethernet segments. For information about Ethernet security card, please refer to 7.11, “8260 Ethernet Security Daughter Card” on page 121.

- Support for port redundancy

  You can set up redundancy between two links on the same module or two different modules. Note that port redundancy is supported between different types of modules. For example, you can set a 10Base-T port on an 8260 Ethernet 20-Port 10Base-T Module to be a redundant port for a port on an 8260 Ethernet 10-Port 10Base-FB Module.

- Support for non-10Base-T compliant devices

  This module allows you to disable link integrity which allows connection to some equipment that does not conform to the 10Base-T standard.

When designing Ethernet segment consisting of the 20/40-port 10Base-T modules, you must use the following *Equivalent Distances* for this module:

Table 18. Equivalent Distances for 20/40 10Base-T Modules

8260 Module	Equivalent Distance (meters)
24-port 10Base-T Module	585
Incoming signal to TP port	420
Outgoing signal to TP port	165

Figure 69 on page 108 shows the front view of the 20/40-port 10BASE-T modules. As can be seen, these modules provide you with LED Indicators on the front panel that allow you to monitor the status of the module and the individual ports.

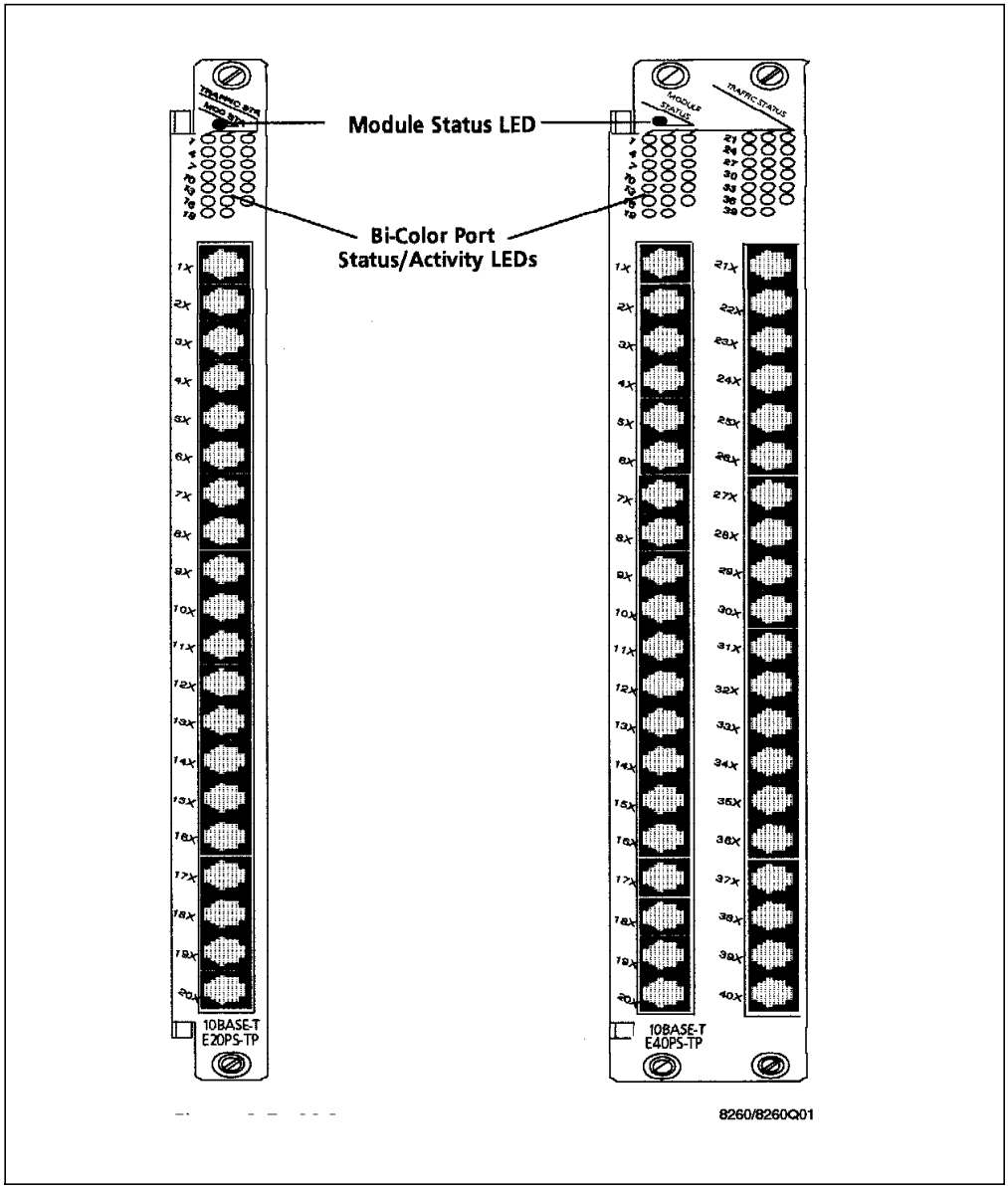


Figure 69. Front View of 20/40-Port 10Base-T Modules

Table 19 describes the meaning of these LEDs:

Table 19 (Page 1 of 2). 20/40-Port 10Base-T Module LED Descriptions

LED Name	Color	State	Description
Module Status	Green	On	Module powered up OK
		Off	No Power.
		Blinking	Module failed self diagnostics
Activity	Yellow	On	Constant activity on the port
		Off	No packets received on the port
		Blinking	Normal activity on the port

Table 19 (Page 2 of 2). 20/40-Port 10Base-T Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
Status	Green	On	Port enabled and link OK
		Off	Port disabled.
		1 Blink	Link failure on the port
		2 Blinks	Port partitioned

Figure 70 shows the side view of the 20/40-port 10Base-T modules. As can be seen, in addition to the 8 isolated segments and the mounting for two E-MACs, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored. For more information, please refer to 4.2.4.4, " Configuring DMM Device" on page 50.

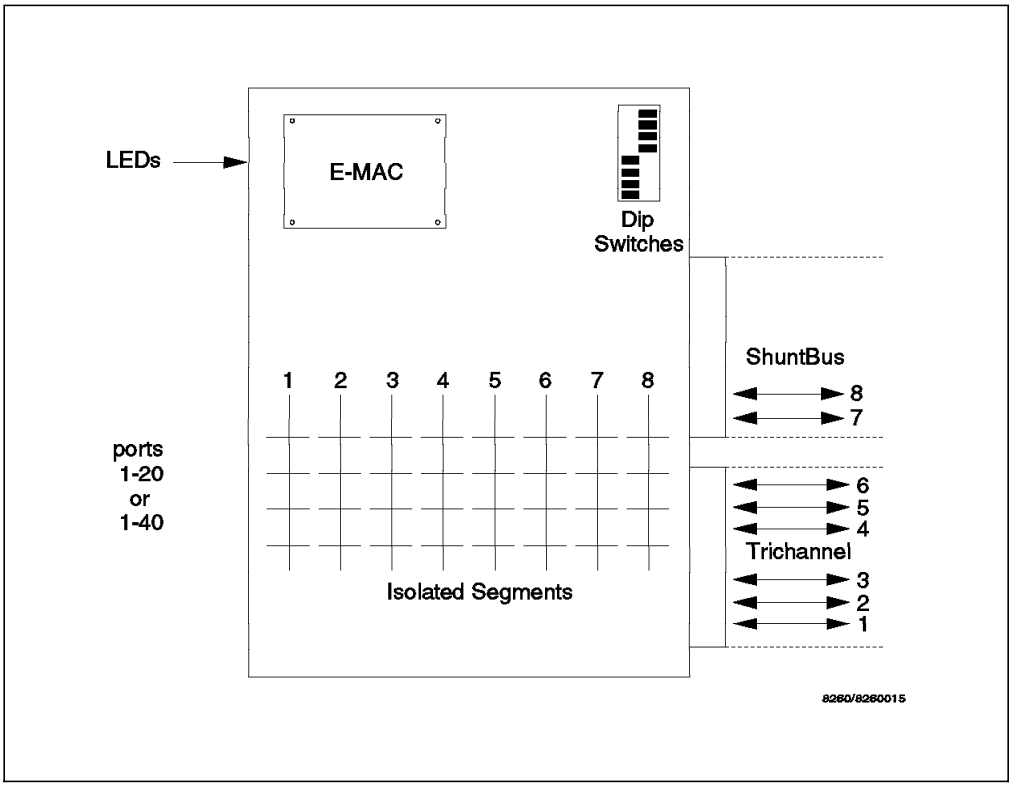


Figure 70. 20/40-Port 10Base-T Module Side View

The expanded view of the DIP switches is shown in Figure 71 on page 110.

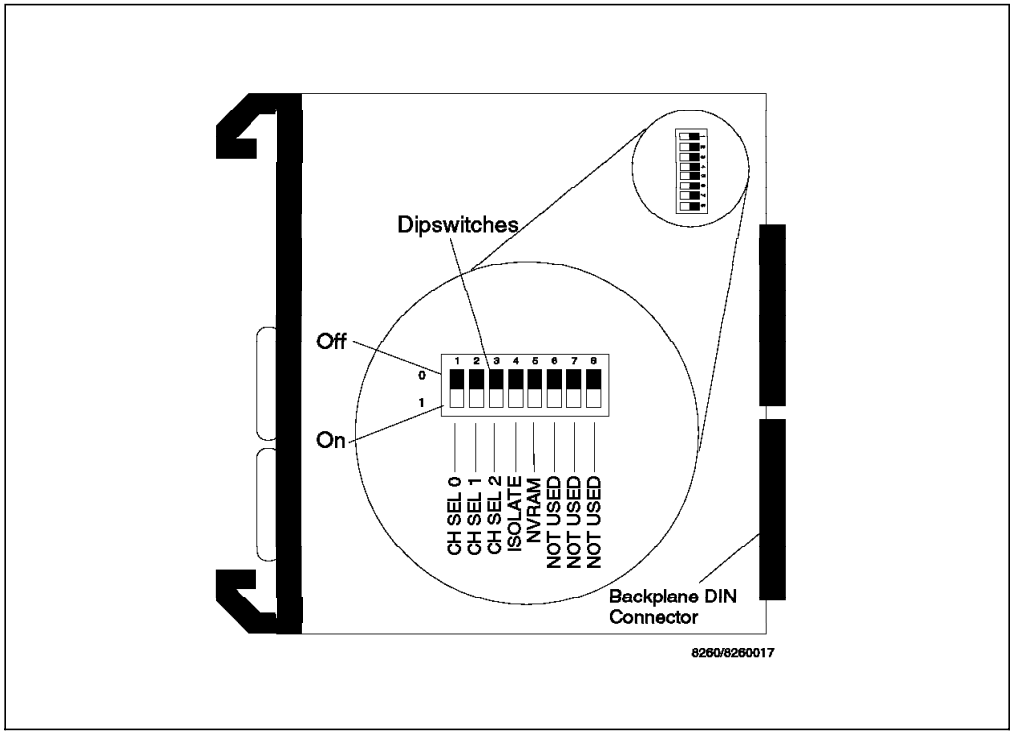


Figure 71. 20/40-Port 10Base-T DIP Switches

The DIP switches let you perform the following:

- Use DIP switch positions 1 through 4 to assign all the ports on the module to one of the backplane segments or an isolated-1 segment. Note that when using DIP switches, all the ports will be assigned to the same segment, so you cannot do per-port switching when using DIP switches for configuring the 8260 modules.

  Table 20 shows the meaning of the settings for DIP switches 1 thru 4:

Table 20. 20/40-Port 10Base-T Module DIP Switch Settings

Network Selection	Switch 1	Switch 2	Switch 3	Switch 4
Ethernet_1	OFF	ON	ON	ON
Ethernet_2	ON	OFF	ON	ON
Ethernet_3	OFF	OFF	ON	ON
Ethernet_4	ON	ON	OFF	ON
Ethernet_5	OFF	ON	OFF	ON
Ethernet_6	ON	OFF	OFF	ON
Ethernet_7	OFF	OFF	OFF	ON
Ethernet_8	ON	ON	ON	OFF
Isolated_1	ON	ON	ON	ON

  By default, these modules are shipped from the factory with the DIP switches set for Ethernet_1.

- Use DIP switch position 5 to choose if the module is going to use the Non-Volatile RAM (ON position) or DIP switch settings (OFF position) for its configuration. Note that if there is a management module installed in the 8260, this DIP switch determines which configuration (NVRAM or DIP switch

setting) will be sent to the management module. The actions taken by the management module, upon receipt of this information are described in 4.2.4.4, " Configuring DMM Device" on page 50. By default, DIP switch 5 is set to NVRAM.

7.6 Configuring the 20/40-Port 10Base-T Modules

To configure the 20/40-port 10Base-T modules you must do the following:

- Select network for each port

  Each port can be assigned to one of the 8 Ethernet segments on the backplane or one of the 8 isolated segments on the module. Note that the ports can be connected to a maximum of eight backplane and/or isolated segments simultaneously.

  The port assignment can be done via onboard dip switches or the following management module command:

  ```
  SET PORT {slot.port} NETWORK {network}
  ```

  Note

  When using DIP switches on these modules, it is only possible to assign all the ports to the same network. This network can be one of the 8 Ethernet segments on the backplane, or isolated-1.

- Enable/disable ports

  Each port on the 20/40-port 10BASE-T modules can be enabled/disabled independently from the other ports. You can use the following management module command to enable/disable a port:

  ```
  SET PORT {slot.port} MODE {enable|disable}
  ```

- Enable/disable auto-polarity

  This feature enables the 20/40-port 10BASE-T modules to automatically switch the polarity of the twisted-pair cabling in case the polarity of the cabling has been erroneously reversed during the cable assembly. To enable auto polarity detection and reversal on each port, you can use the following management module command:

  ```
  SET PORT {slot.port} AUTO_POLARITY {enable|disable}
  ```

- Set port redundancy

  The port redundancy feature allows you set redundancy between two ports. The two ports can be on the same or different modules and can be of the same or different types. For example, a 10Base-T port can be defined to be a redundant port for a 10Base-FB port. Port redundancy is allowed between the 8250 and the 8260 ports. You can use the following management module command to set port redundancy:

  ```
  SET PORT {slot.port} MODE REDUNDANT {slot.port}
  ```

  When the port redundancy is no longer required, you can use the following management command to set the port to operate in non-redundant mode:

  ```
  SET PORT {slot.port} MODE NON-REDUNDANT
  ```

- Set port squelch

  The 20/40-port 10BASE-T modules allow you to establish either normal (high) or low (sensitive) squelch level for each port. The normal squelch level

allows the port to receive signals compliant with 10Base-T standard. Low squelch level allows the port to receive weaker signals, enabling you to have longer distances, but increases the risk of losing packets due to the impulse noise. The maximum distances supported for UTP and STP cabling under different squelch settings are shown in Table 21.

Table 21. Maximum Distances for 20/24-Port 10Base-T Modules

Cable Type	Normal Squelch	Low Squelch
STP	100 M	300 M
UTP 22	100	200
UTP 24	100	150

The following management command is used to set the squelch setting for the ports:

```
SET PORT {slot.port} SQUELCH {normal|low}
```

Note that the modules are shipped from the factory with the squelch level set to normal.

- Enable/disable link integrity

  To connect older equipment, that does not fully comply with the 10Base-T standard, to this module, you may use the following management module command to disable the link integrity:

  ```
  SET PORT {slot.port} LINK_INTEGRITY {enable|disable}
  ```

- Enable/disable port alert

  You may use the following command to enable/disable the sending of port up and down alerts from the individual ports on this module:

  ```
  SET PORT {slot.port} ALERT_FILTER {enable|disable}
  ```

  This command may be used to allow you to monitor the status of the crucial ports on your network while the alerts from the other ports are disabled.

- Enable/Disable remote Diagnostics

  The Remote Diagnostics feature allows this module to detect certain unusual failure conditions when used in conjunction with the IBM Fault-Tolerant 10Base-T Transceiver. You can use the following management command to enable/disable remote diagnostics:

  ```
  SET PORT {slot.port} MODE {remote_diagnostics|non_remote_diagnostics}
  ```

Note

The 10Base-T specification specifies a minimum of 31 collisions prior to partitioning of a port. The 8260 Ethernet 24-Port 10Base-T Module automatically partitions a port when more than 63 collisions are detected on that port. This value cannot be changed by the users.

7.7 8260 Ethernet 10-Port 10Base-FB Module

The 8260 Ethernet 10-Port 10Base-FB Module is a 10-port module that complies with the 10Base-FB standard and supports backbone and to-the-desk connectivity over fiber optic cabling.

To provide backbone connectivity, the 8260 Ethernet 10-Port 10Base-FB Module can be connected via a fiber cable to one of the following:

- An 8260 using 8260 10-Port 10Base-FB module
- An 8260 using 8250 2/4-port 10Base-FB module
- An 8250 using 8250 2/4-port 10Base-FB module
- A third party hub using a 10Base-FB compliant module

This module supports 50/125, 62.5/125, 85/125 or 100/140 micron duplex fiber rated at 150 MHz or better and can be ordered with either ST, FC or SMA-type connectors. You should use different part numbers and feature codes when ordering this module with different connector types.

In general, on 62.5 micron cable, you can go up to a maximum of 4000 meters (when the module is set to operate at high power mode) point-to-point using 8250 and/or 8260 10Base-FB modules. However, if you have poor quality cable, splices or many patch panels, you may have to reduce this distance.

The workstations connecting to this module should use either the IBM 10Base-FB Transceivers or any transceiver which fully complies with the 802.3 10Base-FB standard.

The 8260 Ethernet 10-Port 10Base-FB Module provides the following features:

- Per-port switching

  Each port can be connected to one of the eight segments on the backplane. Also, the module provides four isolated segments to which the individual ports on the module can be attached. These isolated segments can be used to set up segments consisting of the users attached to that module without using any backplane resource.

  Note

  The 8260 Ethernet 10-Port 10Base-FB Module supports any combination of backplane and isolated segments. So, you have the freedom to assign any of the 10 ports to any of the backplane or isolated segments.

- Support for 1 E-MAC

  This module provides the mounting for one E-MAC. The E-MAC can be assigned to any of the Ethernet segments on the backplane, or any of the isolated segments on this module. Note that the E-MAC mounted on this module cannot collect per-port or per-module statistics about the 8250 modules.

- Support for 1 Ethernet security card

  In addition to mounting for the E-MAC, this module provides the mounting for one Ethernet security card. The Ethernet Security card provides for eavesdropping and intrusion control for your Ethernet segments. For

information about the Ethernet security card, please refer to 7.11, “8260 Ethernet Security Daughter Card” on page 121.

- Support for port redundancy

  You can set up redundancy between two links on the same module or two different modules. Note that port redundancy is supported between different types of modules. For example, you can set a 10Base-T port on an 8260 Ethernet 24-Port 10Base-T Module to be a redundant port for a 10Base-FB port on the 8260 Ethernet 10-Port 10Base-FB Module.

When designing an Ethernet segment consisting of the 8260 Ethernet 10-Port 10Base-FB Module, you must use the following *Equivalent Distances* for this module:

Table 22. Equivalent Distances for Ethernet 10Base-FB Module

8260 Module	**Equivalent Distance (meters)**
24-port 10Base-T Module	190
Incoming signal to TP port	140
Outgoing signal to TP port	50

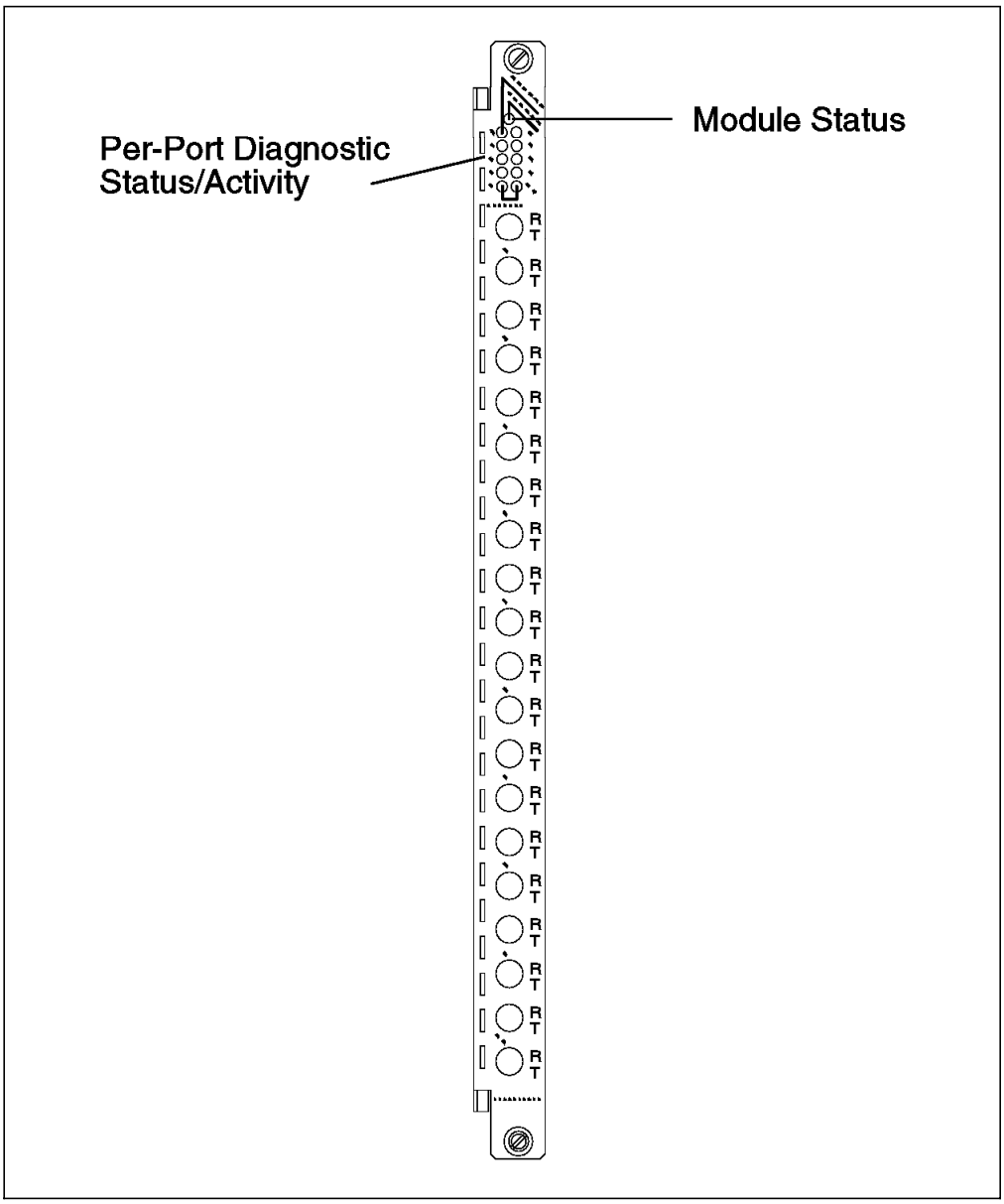


Figure 72. Front View of 10-Port 10Base-FB Module

Figure 72 shows the front view of the 8260 Ethernet 10-Port 10Base-FB Module. As can be seen, the 8260 Ethernet 10-Port 10Base-FB Module provides you with LED indicators on the front panel that allow you to monitor the status of the module and the individual ports. Table 23 describes the meaning of these LEDs:

Table 23 (Page 1 of 2). 10-Port 10Base-FB Module LED Descriptions

LED Name	Color	State	Description
Module Status	Green	On	Module powered up OK
		Off	No Power.
		Blinking	Module failed self diagnostics

Table 23 (Page 2 of 2). 10-Port 10Base-FB Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
Activity	Yellow	On	Constant activity on the port
		Off	No packets received on the port
		Blinking	Normal activity on the port
Status	Green	On	Port enabled and link OK
		Off	Port disabled.
		1 Blink	Link failure on the port
		2 Blinks	Jabber
		3 Blinks	Port partitioned
		4 Blinks	Remote fault
		5 Blinks	Invalid data

Figure 73 shows the side view of the 8260 Ethernet 10-Port 10Base-FB Module. As can be seen, in addition to the 4 isolated segments and the mounting for the E-MAC, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored.

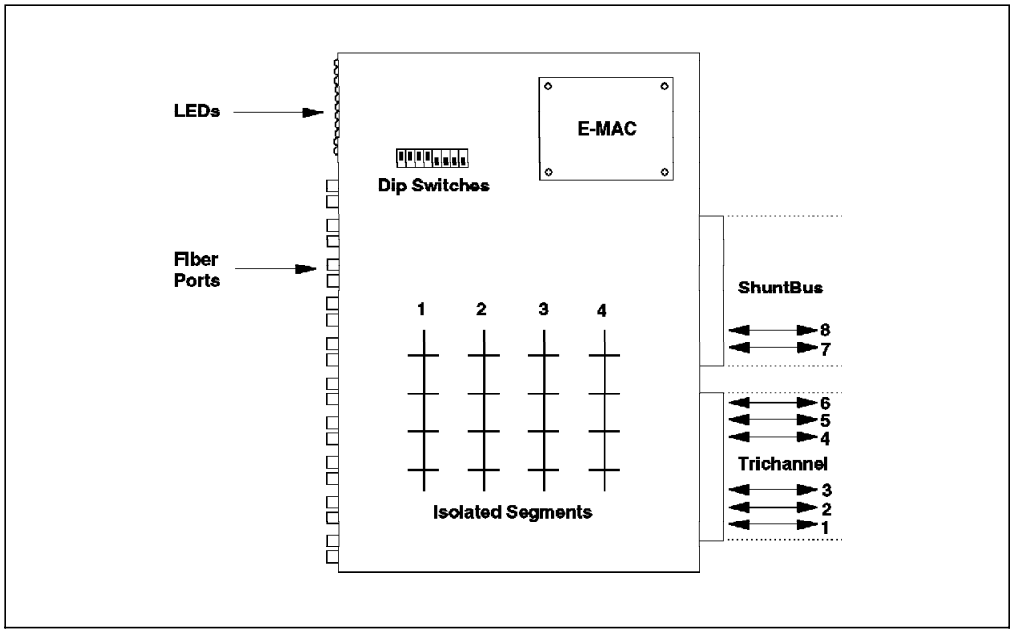


Figure 73. 10-Port 10Base-FB Module Side View

The expanded view of the DIP switches is shown in Figure 74 on page 117.

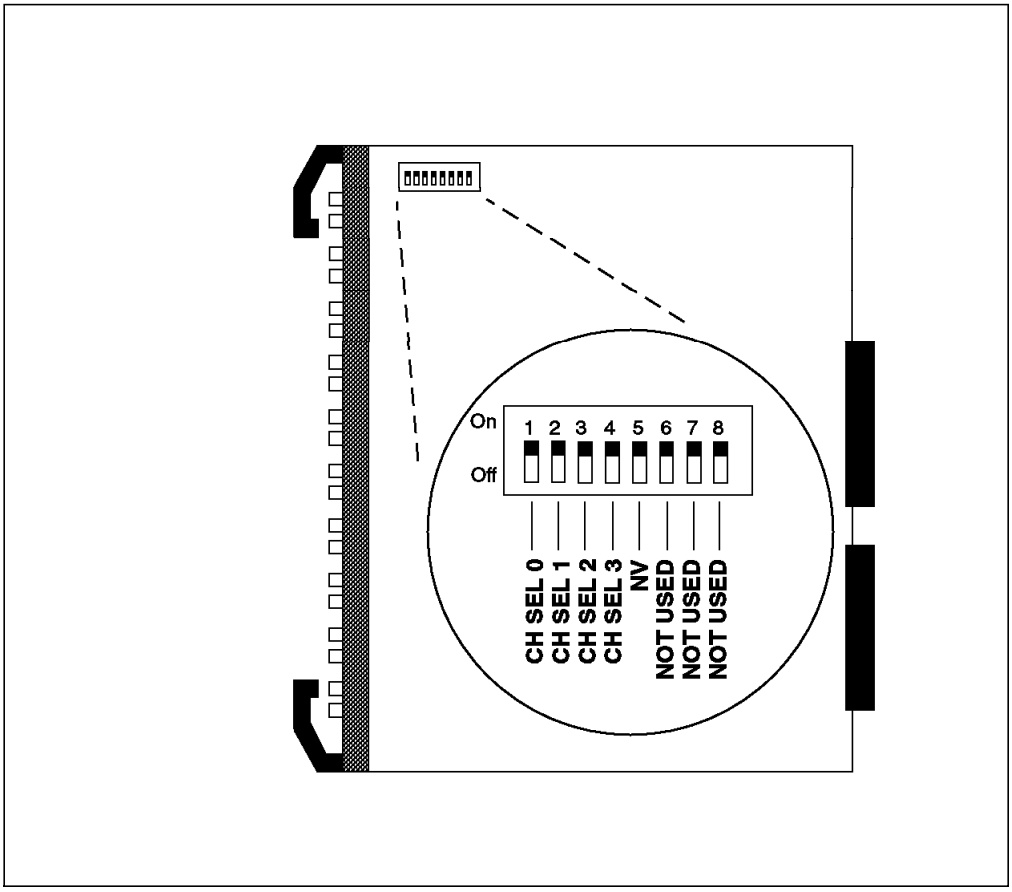


Figure 74. 10-Port 10Base-FB DIP Switches

The DIP switches let you perform the following:

- Use DIP switch positions 1 through 4 to assign all the ports on the module to one of the backplane segments or isolated-1 segment. Note that when using DIP switches, all the ports will be assigned to the same segment, so in effect, you cannot do per-port switching.

  Table 17 on page 103 shows the meaning of settings for DIP switches 1 thru 4:

Table 24. 10-Port 10Base-FB Module DIP Switch Settings

Network Selection	Switch 1	Switch 2	Switch 3	Switch 4
Ethernet_1	ON	ON	ON	ON
Ethernet_2	OFF	ON	ON	ON
Ethernet_3	ON	OFF	ON	ON
Ethernet_4	OFF	OFF	ON	ON
Ethernet_5	ON	ON	OFF	ON
Ethernet_6	OFF	ON	OFF	ON
Ethernet_7	ON	OFF	OFF	ON
Ethernet_8	OFF	OFF	OFF	ON
Isolated_1	ON	ON	ON	OFF

By default, the module is shipped from the factory with the DIP switches set for Ethernet_1.

- Use DIP switch position 5 to choose if the module is going to use the Non-Volatile RAM (ON position) or DIP switch settings (OFF position) for its configuration. Note that if there is a management module installed in the 8260, this DIP switch determines which configuration (NVRAM or DIP switch setting) will be sent to the management module. The actions taken by the management module, upon receipt of this information are described in 4.2.4.4, " Configuring DMM Device" on page 50. By default, the DIP switch 5 is set to NVRAM.

7.8 10Base-FB Module Usage

Figure 75 provides an example of the usage of the 8260 Ethernet 10-Port 10Base-FB Module.

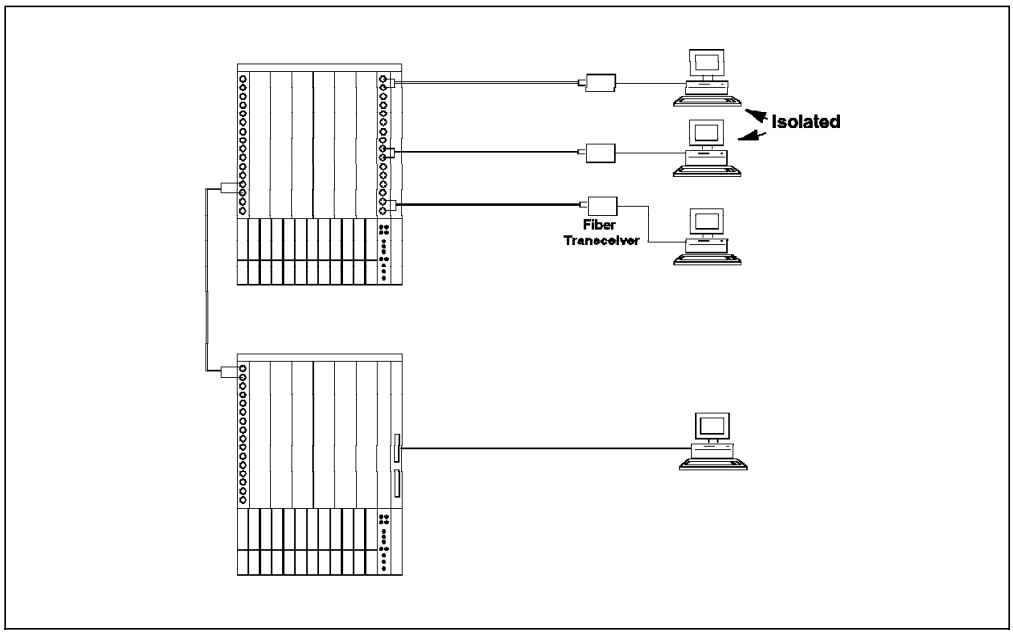


Figure 75. 10-Port 10Base-FB Module Usage

7.9 Configuring the 10Base-FB Module

To configure the 8260 Ethernet 10-Port 10Base-FB Module you must do the following:

- Select a network for each port

  Each port can be assigned to one of the 8 Ethernet segments on the backplane or one of the 4 isolated segments on the module.

  The port assignment can be done via onboard dip switches or the following management module command:

  ```
  SET PORT {slot.port} NETWORK {network}
  ```

Note

Using DIP switches on the 8260 Ethernet 10-Port 10Base-FB Module, it is only possible to assign all the ports to the same network. This network can be one of the 8 Ethernet segments on the backplane, or isolated-1.

- Enable/disable ports

  Each port on the 8260 Ethernet 10-Port 10Base-FB Module can be enabled/disabled independently from the other ports. You can use the following management module command to enable/disable a port:

  ```
  SET PORT {slot.port} MODE {enable|disable}
  ```

- Set port redundancy

  The port redundancy feature allows you to set redundancy between two ports. The two ports can be on the same or different modules and can be of different types. For example, a 10Base-T port can be defined to be a redundant port for a 10Base-FB port. Also, port redundancy is allowed between the 8250 and the 8260 ports. You can use the following management module command to set port redundancy:

  ```
  SET PORT {slot.port} MODE REDUNDANT {slot.port}
  ```

  When configuring port redundancy, the redundancy should be enabled for one end of the link only. This is shown in Figure 76.

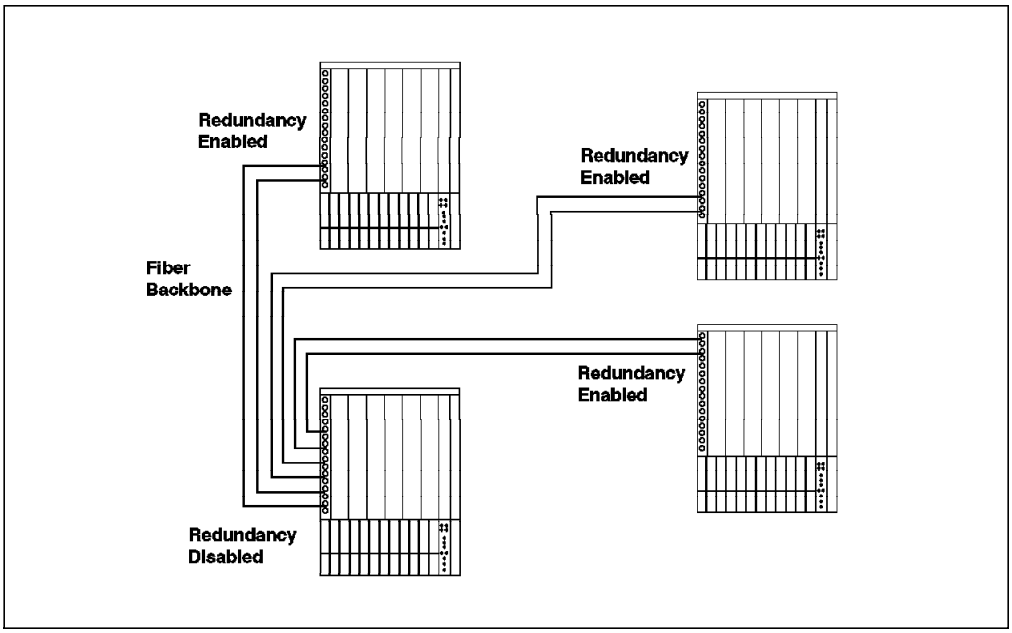


Figure 76. Configuring Port Redundancy for 8260 Ethernet Modules

When port redundancy is no longer required, you can use the following management command to set the port to operate in non-redundant mode:

```
SET PORT {slot.port} MODE NON-REDUNDANT
```

- Enable/disable port alert

  You may use the following command to enable/disable the port up and down alerts received from the individual ports on this module:

  ```
  SET PORT {slot.port} ALERT_FILTER {enable|disable}
  ```

This command may be used to allow you to monitor the status of the crucial ports on your network while the alerts from the other ports are disabled.

- Set optical power

  Each port on this module can be set to operate at high or normal power. When operating at high power mode, the fiber distance between the two modules and the module or the transceiver can be as far as 4000 meters. Please note that you must enable high power mode at both ends to achieve the maximum possible distance. To set the power mode, you can use the following management command:

  ```
  SET PORT {slot.port} HIGH_POWER {enable|disable}
  ```

7.10 8260 Ethernet Modules Summary

The following table provides a summary of the functions supported by the 8260 Ethernet modules.

Table 25. 8260 Ethernet Modules Summary

Module	24-Port 10Base-T	10-Port 10Base-FB	20-Port 10Base-T	40-Port 10Base-T
Feature Code	1024	1110, 1210, 1610	1020	1040
Daughter Cards Supported	1	1	2	2
I/O Modules	N/A	N/A	N/A	N/A
Number of Ports	24	10	20	40
Type of Ports	Telco	ST, FC, SMA	RJ-45	RJ-45
Switching Supported	Port	Port	Port	Port
Number of Slots Used	1	1	1	2
Number Backplane Networks Accessible	8	8	8	8
Number of Isolated Networks Accessible	8	4	8	8
Number of Segments Supported Simultaneously	Any Combination of 6	Any Combination	Any Combination of 8	Any Combination of 8
Cabling Supported	UTP Cat 3 and Above	Multi-mode Fiber	UTP & STP	UTP & STP
Security Card Support	Yes - Not on Isolated Networks	Yes - Not on Isolated Networks	Yes - Not on Isolated Networks	Yes - Not on Isolated Networks
Port Redundancy	Yes	Yes	Yes	Yes
Network Statistics Supported Without Monitoring Card	No	No	Repeater MIB	Repeater MIB
Other Notes		Fiber supported - 50/125, 62.5/125, 85/125, 100/140		

7.11 8260 Ethernet Security Daughter Card

The 8260 Ethernet Security Card (E-SEC) is a daughter card that allows you to provide security on any Ethernet network to which this card is attached. You can install this card on any Ethernet media module or the 8260 DMM with Ethernet Carrier (EC-DMM).

Note

Security features provided by this card are only applicable to the Ethernet ports on the 8260 modules. Therefore, this card cannot be used to provide security for the Ethernet ports on the 8250 modules installed on your 8260, even if they are assigned to the Ethernet network protected by the Ethernet security card.

Once assigned to an Ethernet network, the E-SEC card can be used to provide the following security features for that network:

- Intrusion protection

  This feature allows only the authorized users for each port to transmit data on that port. If an unauthorized user is detected on a port, the E-SEC card may be configured to perform one or more of the following:

  – Report the time and port on which the intrusion took place along with the MAC address of the intruder.

  – Jam the intruder's port so that the intruder is not able to exchange data with the other stations on the network.

  – Disable the port to which the intruder is connected.

  Authorized users on each port are known to the E-SEC card via the *network security address table*. The contents of this table can be created and/or modified using *manual* and/or *auto-learning* procedures as described in 7.11.2, "Configuring the Security Module" on page 124.

  Each entry in the network security address table contains the 8260 slot and port number as well as the MAC address of the station authorized to transmit data on that port. You may define as many authorized users as you wish for each port. However, the total number of users defined for each network, that is the total number of entries allowed in the network security address table is limited to 1,000 entries.

  Note: When performing intruder protection, you may configure the E-SEC card to either check only the MAC address of the sending adapter, or both the MAC address and the port to which the sending station is attached.

- Eavesdropping protection

  This feature prevents unauthorized users from examining the contents of packets destined for another port by preventing all the nodes except the intended recipient from receiving the packets transmitted on the network. This enables you to ensure that unauthorized network tracing tools will not be able to listen and trace the network traffic.

Note that the eavesdropping and intrusion protection functions can be enabled or disabled separately for each port. Also, various ports on a single network may have different security settings. For example, in a single network, some ports may have both eavesdropping and intrusion protection enabled, while other

ports may have one of these two features enabled and finally the last group of ports which may have no security at all.

Details of configuring security features are described in 7.11.2, “Configuring the Security Module” on page 124.

7.11.1 Operation of Security Card

When transmitting a packet, the 8260 Ethernet modules will use either *method 2* or *method 3* as described in 2.2, “Ethernet Segments on the Backplane” on page 15 for communication across the backplane. In both these methods:

1. The data packet will be transmitted over the Data In NRZ pin and
2. The slot ID and port ID are transmitted in serial over the Serial ID pin

The E-SEC card will listen to the transmitted packets over Data In NRZ pin. Since each Ethernet packet carries the source and the destination address of the communicating stations, by monitoring the contents of the transmitted packets over the Data In NRZ pin, the E-SEC card learns who the packet is coming from and who the intended recipient is. The E-SEC card also monitors the Serial ID pin, which allows it to learn which port is sending the transmitted packet. The monitoring of these two pins, allows the E-SEC card to learn the following:

- Source address of the packet
- Destination address of the packet
- The port transmitting the packet

This information, in conjunction with the contents of the network security address table allows the E-SEC card to perform both intrusion and eavesdropping protection.

The following sections describe the theory of operation for each security feature.

7.11.1.1 Intrusion Protection

When performing intrusion protection on a port, the E-SEC card will check the source address of the packet and its port ID against the network security address table entries. If a match is found, the transmitting station is an authorized user. If no match is found, the transmitting station is not authorized to transmit on the network. Once the E-SEC card has determined the authorization of the transmitting station, it immediately sends a *security message* to all the media modules attached to that network segment protected by the E-SEC card. This security message will instruct the media modules to either *pass* or *jam* the transmitted packet on their ports.

Note: The security message is sent on a per packet basis to all the 8260 ports in the hub which are attached to the segment to which the E-SEC card is assigned. The security message will be sent on the Serial ID pin.

When doing intrusion protection only, the same security signal (pass or jam) will be sent to all the ports. If the transmitting station is authorized, the security message will instruct all the media ports to pass the transmitted packet to the stations attached to them. If the transmitting station is not authorized, the security message will instruct all the other ports to jam the transmitted packet.

When the jamming signal is received by an 8620 module for a port, the module will transmit a packet consisting of 0s and 1s (instead of the actual packet) to the

station attached to that port. The transmission of the jammed packet will last the same length of time as the original data packet. Stations that receive a jammed packet will discard it because the CRC (Cyclic Redundancy Check) field of the packet is incorrect.

To perform intrusion control, the E-SEC card must perform the following:

1. Determine the source address of the station transmitting the data. This means that the transmitting station must be allowed to transmit the following portions of the Ethernet packet:
   - Preamble (56 bits)
   - Starting delimiter (8 bits)
   - Destination address (48 bits)
   - Source address (48 bits)
2. Once the source address of the transmitting station is determined, the E-SEC card will search the network security address table to see if the station is authorized to transmit on that port. The time to search the network security address table is equivalent to 11 bit-times.
3. The E-SEC card will send the security message (pass or jam) to all the 8260 ports which are attached to that segment. It takes 16 bit-times for the E-SEC card to send this message.
4. The media module will process the security message and start jamming or passing the packet. This process takes 8 bit-times.

As can be seen, from the time that the source address of the frame is seen by the E-SEC card, it takes 35 bit-times to start jamming or passing the packets. This means that the transmitting station will be able to send 35 bits of the packet from the end of source address to the stations before the jamming process can stop an unauthorized station. This 35 bits includes 16 bits of type/length field and 19 bits of user data.

7.11.1.2 Eavesdropping Protection

To perform eavesdropping protection, the E-SEC card must perform the following:

1. Determine the destination address of the station transmitting the data. This means that the transmitting station must be allowed to transmit the following portions of the Ethernet packet:
   - Preamble (56 bits)
   - Starting delimiter (8 bits)
   - Destination address (48 bits)
2. As soon as the E-SEC card receives the destination address within the packet, it searches the network security address table to determine the port to which the intended recipient is connected. This process takes 8 bit-times.
3. The E-SEC module transmits security messages to media modules attached to that segment protected by the E-SEC card, to instruct them to jam all the ports except the port to which the destination station is attached. This process takes 16 bit-times.
4. The media modules will process the security message and jam or pass the packet. This process takes 8 bit-times.

The entire process of eavesdropping protection takes 32 bit-times from the time the E-SEC card receives the destination address field in the packet.

7.11.2 Configuring the Security Module

To be able to use the security module you must perform the following steps:

1. Assign the security module to the backplane segment on which you want to use the security feature. The following command is an example of how to assign the security card, which is mounted on our 10-port 10Base-F module which is installed in slot 7, to Ethernet_3 segment:

   ```
   8260A> set module 7.2 network ethernet_3
   ```

2. Use the following command to display the current security settings for your network:

   ```
   8260A> show security network ethernet_3
   ```

   This command is necessary to determine the settings of various security parameters in your network. Figure 77 shows the default security settings when you first install the E-SEC module in your hub and assign it to a segment.

```
8260A> show security network ethernet_3

ETHERNET_3 Network Security Configuration
--------------------------------------------------------------------------------
Securing Module:              Slot 07.02 Version v1.00
                              E-SEC: Ethernet Private Line Card

Operational Mode              DISABLED
Administrative Mode           DISABLED

Auto-learning:                ENABLED
Eavesdrop Protection:         DISABLED

Intruder Detection:                       Intruder Actions:
  Source Address Checking:    DISABLED    Intruder Jamming:           DISABLED
  Source Port Checking:       DISABLED    Intruder Reporting:         DISABLED
                                          Intruder Port Disabling:    DISABLED

8260A>
```

Figure 77. Default Security Settings

3. Build the network security address table so it contains information about all the stations which are authorized to access your network and their corresponding port. The network security address table can be built automatically and/or manually. We recommend the following procedure to build this table:

   a. Build the initial table using the auto-learning feature of the E-SEC module. To do so, you must do the following:

      - Enable auto-learning feature for each port on which you want the E-SEC card to learn the MAC addresses automatically. You can use the following example for each port:

        ```
        8260A> set security port 2.15 auto-learning enable
        ```

- Enable auto-learning for your Ethernet segment using the following example:

  ```
  8260A> set security network ethernet_3 auto-learning enable
  ```

- Although the port and network auto-learning is enabled, the E-SEC module will not auto-learn MAC addresses attached to each port until you enable the security mode for the segment using the following example:

  ```
  8260A> set security network ethernet_3 mode enable
  ```

  At this stage, the E-SEC module learns the addresses of all the stations attached to the ports for which you have enabled the auto-learning option.

- Review the contents of the network security address table using the following command:

  ```
  8260A> show security address_table {all | group | port}
  ```

  The output from this command for our network is shown in Figure 78.

```
----- -------- ------------------- ---------------- ----------------------
02.16 ENABLED  OKAY                ETHERNET_3

8260A> show security port 2.16 verbose


Security Port Table Display for Module 1 E24PS-6/8:

Port   AutoLearn  FailSafe  Group_A  Group_B  Intruder_Check  Jamming
----   ---------  --------  -------  -------  --------------  -------
02.16  ENABLED    DISABLED        0        0  DISABLED        ENABLED

8260A> set security network ethernet_3 mode enable
ETHERNET_3 Administrative Mode set to ENABLED.

8260A> show security address_table all

Entry   Port    Group_Code   MAC_Address
-----   -----   ----------   -----------------
   1.    2.8                08-00-5a-61-58-cf
   2.    2.15               10-00-5a-d4-b0-8c
   3.    2.12               10-00-5a-82-59-32
   4.    2.16               10-00-5a-82-5a-6a

8260A>
```

Figure 78. Network Security Address Table

- Once you are satisfied that all the desired entries have been learned, you must stop the auto-learning on the network using the following command:

  ```
  8260A> set security network ethernet_3 auto-learning disable
  ```

  Note: If you do not disable auto-learning, any deletions that you may do in this table will be rendered useless as the E-SEC module will learn the addresses again.

b. Add or delete entires to the network security table using the manual process. For example, we deleted the entry for port 2.12 as we did not

wish the station shown in Figure 78 for this port to be able to access our network. The following command was used to delete this entry:

```
8260A> set security address_table address 10-00-5a-82-59-32 delete
```

c. Once you are satisfied that the network address table contains all the desired entries, you can save this table on the non-volatile RAM of the E-SEC module using the following command:

```
8260A> save security address_table
```

4. Enable port jamming on each port using the following example:

```
8260A> set security port 2.15 jamming enable
```

Port jamming enables you to prevent intruders from accessing the network by jamming the frames originated from an intruder. It also allows you to prevent eavesdropping on those ports.

Note: Port jamming is enabled by default on all the ports.

5. If you are planning to perform eavesdropping protection, you must enable this option for the network using the following example:

```
8260A> set security network ethernet_3 eavesdrop_protection enable
```

This command prevents all the ports for which you have enabled port jamming from using tracing tools to listen to the network traffic.

Note: When eavesdropping is enabled, all the ports will still be able to receive broadcast messages.

6. For each port on which you plan to perform intruder checking, you must perform the following steps:

a. Enable source address checking for the network using the following example:

```
8260A> set security network ethernet_3 source_address_checking enable
```

This option enables the security card to check the source address in the packets against the contents of the network security address table.

b. Enable source port checking for the network using the following example:

```
8260A> set security network ethernet_3 source_port_checking enable
```

This option enables the security card to check the source port of the packets against the contents of the network security address table.

c. Use the following example to enable intruder checking:

```
8260A> set security port 2.15 intruder_checking enable
```

When you enable intruder checking for a port, the E-SEC card checks each packet's source MAC address against the entries in the network security address table. If the source address does not match one of the authorized stations on that port, the packet is considered an intruder. For the intruder packets, the E-SEC module will take one or more of the actions that are specified in the next steps.

Note: The above parameters allow you to check either the source of the packet or the source and the port of the packet against the contents of the network security address table. If you enable the source address checking but not the source port checking, regardless of the port on which the packet is received, it is regarded as authorized as long as the source MAC address is found in the network security address table.

7. The following actions can be performed by the E-SEC card in case of intruder detection:

   a. Report intrusions by logging information about the intrusion in the intruder table. To enable intruder reporting, you must issue the following command:

      ```
      8260A> set security network ethernet_3 intruder_reporting enable
      ```

      Note: When you enable intruder reporting only, the intruder will still be able to send data on the network, but an entry will be logged in the intruder table to report the intrusion. You can look at the contents of the intruder table using the following command:

      ```
      8260A> show security intruder_table chronological
      ```

      An example of the resulting display is shown in Figure 79.

```
8260A> show security intruder_table
Enter sort by:
8260A> show security intruder_table chronological

Security Intruder Table

Port   Mac Address        Network     Attempts  Time Since Intrusion
----   -----------        -------     --------  --------------------
02.16  10-00-5a-82-5a-6a  ETHERNET_3        19   0d 21h 15m 43s
02.15  10-00-5a-d4-b0-8c  ETHERNET_3         2   0d 21h 28m 10s
8260A>
```

Figure 79. Ethernet Security Intruder Table

      Note: The intruder table is stored by DMM but not in non-volatile RAM. Therefore, the contents of the intruder table will be lost after a reset of DMM.

   b. Jam intruder packets by issuing the following commands in the intruder table. To enable intruder jamming, you must issue the following command:

      ```
      8260A> set security network ethernet_3 intruder_jamming enable
      ```

      Note: This option will jam any packets sent by the intruders. But, the intruder will still be allowed to attempt to send packets on the network.

   c. Disable ports on which an intruder is detected using the following example:

      ```
      8260A> set security network ethernet_3 intruder_port_disabling enable
      ```

      As a result of this option, any port on which an intruder is detected will be disabled automatically, so the intruder will not be allowed to send any other packets on the network.

      To enable transmission of data on the disabled ports, the network administrator must enable the port using DMM commands.

8. You may enable *failsafe* for individual ports attached to a secure network. This parameter instructs the media modules connected to a secure network to expect a security message from the E-SEC card for each transmitted packet. If a security message is not transmitted to the media module, the media module will automatically jam the ports for which the failsafe feature

and port jamming is enabled. You can use the following example to enable the failsafe feature for each port:

```
8260A> set security port 2.15 failsafe enable
```

Chapter 8. 8260 Token-Ring Support

The 8260 token-ring support has been enhanced, compared to the 8250, to provide the following features:

- Active re-timing per port
- Speed detection by media modules
- Beacon recovery by media modules
- Address-per-port mapping

This chapter will cover these features as well as some token-ring architecture background necessary to describe these features. It is beyond the scope of this book to provide detailed information about the token-ring architecture. It is recommended that you refer to the *Token-Ring Network Architecture Reference (SC30-3374)* for more details.

8.1 Token-Ring LAN Overview

In a token-ring LAN environment, all stations are connected in a star-wired ring topology. Each ring can support up to 255 stations. It uses the *token-passing protocol* to enable each station to access the media to transmit data.

8.1.1 Ring Operation

In a token-passing protocol, a token is used to control access to the ring. It is like a passport that grants the holder permission to transfer data to the ring. This token constantly circulates around the ring and is available for any station.

- To transmit data, a station has to capture a token and modify it to indicate that it is transmitting data. The data transmission unit is called a *frame*.
- The frame is sent sequentially from one station to the next physically active station (known as the downstream neighbor) on the ring. Each station upon receiving that frame would check to see whether its MAC address or any of its functional addresses matches that in the destination address of the frame.
- If they match, the station would copy the data and forward the frame to its downstream neighbor.
- As this is a ring, the frame will ultimately return to the originating station, which will remove the frame and release a new token.

This protocol is called a *single-token protocol*, since only one token can circulate on the ring at any time. The architecture provides an option called *early token release*. With this option, the transmitting station will release a token after completing transmission of the data frame but before it receives the header of the transmitted frame. This eliminates the idle time waiting for the header to reappear. This allows for multiple frames, but only one free token on the LAN.

8.1.2 Ring Administration

The token-passing ring protocol provides relatively greater control and management at the medium access control (MAC) level than that provided by the CSMA/CD protocol. All ring administration functions are implemented in the token-ring adapters and the functions are carried out at the MAC level.

8.1.2.1 Active Monitor

In each operational ring, one station assumes the role of the *active monitor*. The process of active monitor selection is described in 8.1.2.2, “Token-Claiming Process” on page 131.

The following are the responsibilities of the active monitor:

- Maintain the master clock

  The active monitor maintains the ring′s master clock. All the other clocks on the ring are synchronized with the active monitor′s clock.

- Ensure proper ring delay

  To ensure that a token is completely transmitted before returning to the originating ring station, the active monitor introduces a 24-bit delay (the length of token) into the ring.

- Initiating neighbor notification

  Every seven seconds, the active monitor broadcasts an Active Monitor Present (AMP) MAC frame to all the stations on the ring. The first station that receives this frame, copies it and sets the address-recognized (A) and frame-copied (C) bit to B′1′. This station, then saves the source address field from the copied frame as its Nearest Active Upstream Neighbor (NAUN). After a period of time called *notification-response time*, this station transmits a Standby Monitor Present (SMP) MAC frame to all the stations on the ring.

  The next downstream station ignores the Active Monitor Present MAC frame (because the A and C bit are set to B′1′), but it copies the Standby Monitor Present MAC frame issued by its NAUN. It then sets the A and C bits to B′1′ and also copies its NAUN from the source address of this MAC frame. This station will, in turn, transmit its own Standby Monitor Present MAC frame.

  In this way, neighbor notification proceeds around the ring with all the stations transmitting their own Standby Monitor Present MAC frame until the active monitor copies the last Standby Monitor Present MAC frame, in which the A and C bit are set to B′0′. At this point, the neighbor notification is considered complete.

  As can be seen, the neighbor notification (which is also referred to as *ring poll*) enables each ring station to learn its NAUN address and to provide its address to its downstream neighbor. This process is used by the TRMM in the 8250 and the token-ring media modules in the 8260 to perform the *address-to-port mapping* which enables them to determine what is the address(s) of station(s) attached to each port. The details of address-to-port mapping are described in 8.10, “Address-to-Port Mapping for Module Switching Modules” on page 160 and 8.11, “Address-to-Port Mapping for Per-Port Switching Modules” on page 164.

- Initiate ring purge process

  Occasionally, the active monitor may need to initiate a *ring purge* process to reset the ring stations, all appropriate timers and release a new token. The

ring purge process may be triggered after detecting the loss of a token, frame, or errors caused by adapter-insertion or adapter-removal operations.

To purge the ring, the active monitor initiates a *Ring Purge MAC frame* broadcast and starts the Ring-purge timer. If the *Ring Purge MAC frame* has not returned to the active monitor when the timer expires, the *token-claiming* process is initiated.

8.1.2.2 Token-Claiming Process

This process is used to elect a new active monitor. Any station who suspects the active monitor is absent can activate this process.

During the process, a *Claim Token MAC frame* is broadcast at a defined interval and the ring station who manages to capture three of its own *Claim Token MAC* frames will be appointed the active monitor.

8.1.3 Ring Errors

In the event of errors or faults, the token-passing protocol has built-in features to automatically reconfigure the ring to identify and bypass the fault and resume operation. This is an advantage over the CSMA/CD protocol.

Each ring station is capable of detecting and reporting any occurrences of errors or faults. Errors can be classified into the following categories:

- Hard error

  Hard errors are permanent faults that stop all normal traffic on the ring. They are usually first detected at the receive side of the next active downstream station from the fault. That ring station will immediately transmit a *Beacon MAC frame* to alert every station. It continues to transmit *Beacon MAC frames* at a specified time interval until its input signal is restored or until it removes itself from the ring.

- Soft error

  Soft errors are defined as intermittent faults that temporarily disrupt normal ring operation. Each station maintains a set of counters to keep track of soft error occurrences. The values of the soft error counters are sent in the form of a *Soft Error Report MAC frame* to the Ring Error Monitor station (for example, Bridge or LAN Manager station) at two-second intervals.

- Isolating error

  Isolating errors are identified because the fault domain is known. A fault domain is the physical section of the segment bounded by two adapter MAC addresses. A beacon is an example of an isolating error.

- Non-isolating error

  Non-isolating errors exist where the fault domain cannot be identified. The origin of these errors cannot be located. A Frame-copied error is an example of a non-isolating error.

8.1.4 Differential Manchester Coding

The 802.5 standard specifies that Differential Manchester coding is used for transmitting data on the ring. With this encoding technique, every bit is comprised of a half-bit time signal at a low or high polarity and other half-bit time signal at the opposite polarity. The mid-bit transition is for clocking only. The direction of the signal's voltage transition will change whenever a "0" bit is transmitted and will stay the same for a "1" bit transmission. Therefore, each bit consists of two half-bits at opposite polarity. This scheme is said to be *DC balanced*. Figure 80 shows the principles of the Differential Manchester coding.

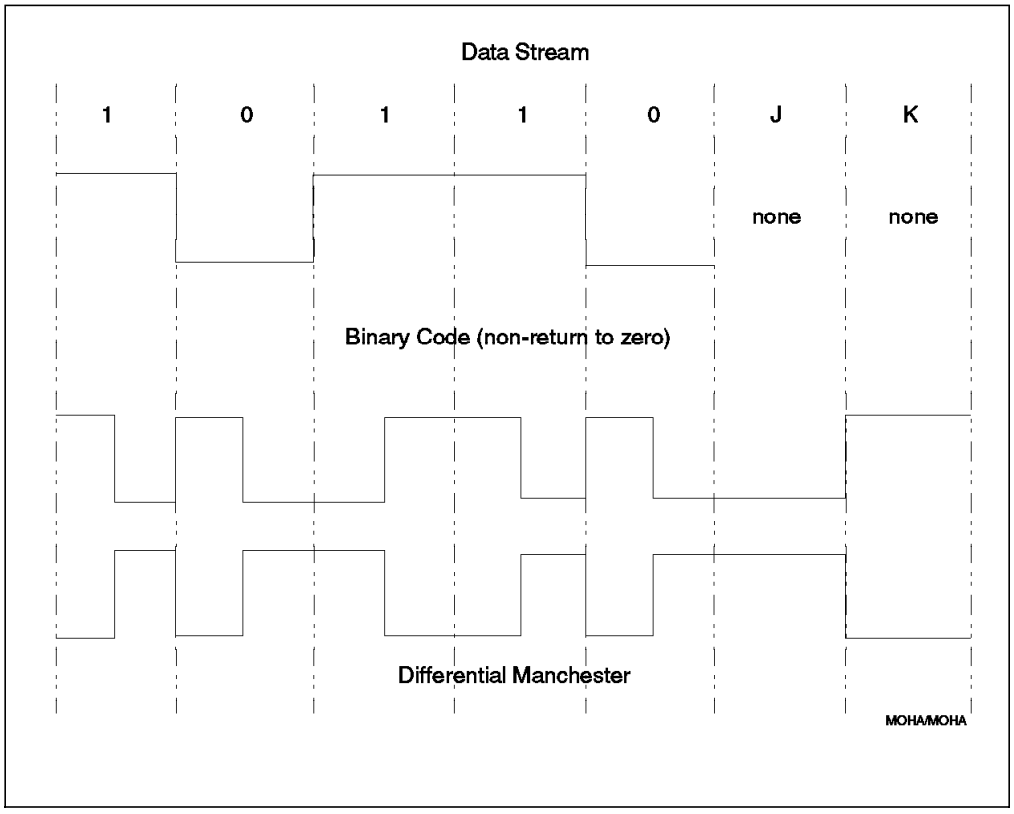


Figure 80. Differential Manchester Coding

To understand the reasons for DC balanced signalling, consider a *baseband* transmission using a simple transmission code such as NRZ (Non-Return to Zero) where during the transmission a "1" bit is represented as a + voltage and a "0" bit is represented as a - voltage (opposite direction of the "1" bit). Depending on the bit stream that is being transmitted with NRZ, it is possible that the line may spend on average more time in one voltage level than the other. In other words, the signal would be electrically *unbalanced*. Since the physical wire has capacitance, the unbalanced signal causes the wire to develop a constant DC voltage across the transmission media, which in turn, causes the transmission media to distort the signal. This phenomenon is called "baseline wander" and the effect of that is to increase the interference caused by one pulse with a subsequent pulse on the transmission media. The result of this interference is that the signal is "smeared" so that the end of one bit, or a group of bits, overlap with the start of the next. This makes an unbalanced coding technique such as NRZ or NRZI unsuitable for high speed transmissions such as 4 or 16 Mbps token-ring networks. The use of Differential Manchester coding technique in token-ring networks would allow us to overcome this problem and have a DC balanced transmission on the media.

The other important point about the Differential Manchester coding is that it uses a higher baud rate (the number of state changes on the transmission media) than the actual data transfer bit rate on the ring, to provide the benefit described above. In fact, the baud rate on the token-ring is twice the data transfer bit rate. On a 4 Mbps token-ring, the baud rate is 8 megahertz. A 16 Mbps token-ring runs at 32 megahertz.

8.1.5 Clock Recovery

The other function that needs to be done in a token-ring environment (which is characterized by a transmission media shared by many stations) is that each receiving station needs to recover a very precise timing from the received bit stream in addition to just reconstructing the bit stream. To do that in a token-ring network, each station could have been designed to have its own independent clock and a large buffer. In this case, every station would have waited to receive the whole frame in its buffer, then it would have used its own clock to generate a new signal which would have been sent to the next station. The receiving station would have repeated this process and so on. The result of this design would have been a very large *ring latency* which would have made it unsuitable for most applications.

In order to minimize ring latency and eliminate the need for a large buffer on each station, the characteristics of Differential Manchester coding (lots of transitions on the transmitted signal) are used so that each station can derive a highly accurate timing source from the received data stream. This timing source is then used by each station to synchronize its clocks with the other stations on the ring. The source timing for all the stations is provided by one of the stations on the ring which is called the *active monitor*.

Note: In any operating ring, one of the stations is elected as the active monitor and the other stations act as *standby monitors* prepared to take over if the active monitor fails. The process of electing an active monitor is called *token-claiming process*. This process is described in 8.1.2.2, “Token-Claiming Process” on page 131.

Because of at least one state transition per bit in Differential Manchester coding, the receiving stations can derive a very stable source timing from the received bit with minimum circuitry and buffering. This results in a minimal delay in each station and hence in the ring. Also, the stability of the derived timing minimizes the *phase jitter* and thus allows more stations to be connected to a single ring segment. However, the phase jitter is not totally removed and requires special attention.

8.1.6 Phase Jitter

Jitter is the generic term given to the difference between the correct timing of the received bit and the timing detected by the received station.

Despite techniques such as Differential Manchester coding, it is impossible for the timing detected by the station to be exactly the same as the correct timing of the received signal. This is because of the characteristics of the transmission media and the high speed (4 or 16 Mbps) of the ring. Some bits will be detected slightly early and some others slightly late. This means that the timing may vary randomly by a small amount on either side of the correct timing.

In some networks, these small differences in the bit timing do not make any kind of difference. But, in the case of token-ring network, the jitter is accumulated as

the signal passes from one station to another and ultimately can result in loss or corruption of data. This is a major reason for the limit on the maximum number of stations supported on a token-ring networks. Note that this limit varies depending on the speed of the ring and type of lobe cables used in attaching the workstations to the hub. Also, there is limitation on the type and the length of lobe cable.

To address these limitations, the 8260 provides the following types of functions on the token-ring media modules:

- Passive port technology
- Active port technology

Before looking at the passive and active port technology as implemented in the 8260, this is an appropriate time to review the signalling used on the 8260 backplane for the token-ring segments.

8.2 8260 Backplane Signalling for TR Segments

The ShuntBus on the 8260 backplane consists of the circuitry to accommodate 10 token-ring segments. The circuitry for each token-ring segment on the backplane forms a physical ring on the backplane with a self-shorting connector at each slot location. Connection from the modules to the backplane can be made by breaking into the ring via these self-shorting connectors. When a token-ring module is installed on the 8260, the backplane rings are broken via the self-shorting connectors and are completed through the circuitry on the modules. These rings can also be bypassed through the inserted module (passively) via the use of relays on the module. This is shown in Figure 81 on page 135.

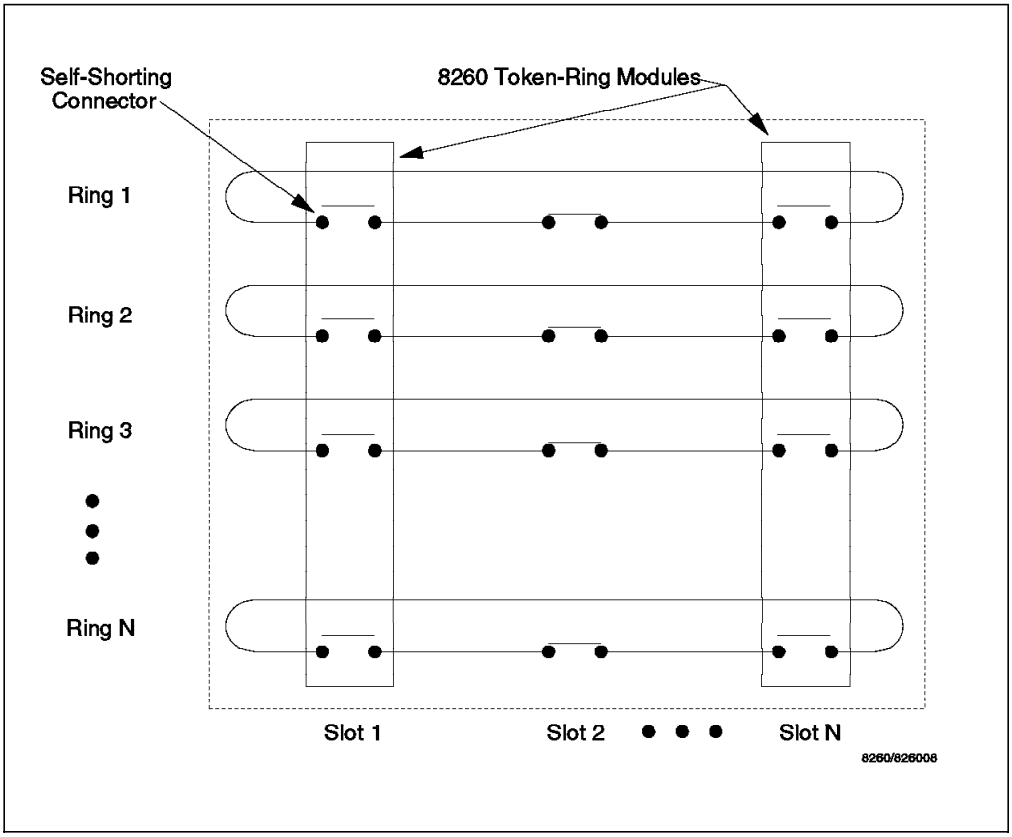


Figure 81. Self-Shorting Relays on the ShuntBus

Once a module is inserted into a slot in the 8260, the ShuntBus connector on the module breaks the shunt on the backplane. It is then the responsibility of the module to restore this connection by using a relay type function. When the module is not configured to connect to a backplane ring, the relay is set such that the backplane shunt is restored. At the same time, the signals transmitted by the module are looped back by the relay to the receive signals. When a module is configured to connect to a backplane ring, the relay connects the input signals from the backplane to receive signals on the lobe and the output signals from the backplane to the transmit signals on the lobe.

Each token-ring interface on the ShuntBus connector uses three shunt pairs to form one token-ring network on the backplane. The three shunt pairs carry a clock and two data signals.

When a token-ring module is inserted into the ring, the 3 shunt pairs connect to 6 signal lines on the module as:

- Clock transmit
- Data_A transmit
- Data_B transmit
- Clock receive
- Data_A receive
- Data_B receive

To reason for two signals for each of the transmit and receive signals is that the bit encoding scheme utilized across the 8260 backplane to support 4 and 16

Mbps operation is different for the two bit-rates. For 4 Mbps operation, the encoding is straightforward. One of the data-signal shunt pairs (Data_A) carries the Differential Manchester encoded bit stream, whereas there is no signal on the other pair (Data_B). The clock shunt pair carries a synchronous clock which is used to sample the Data_A signal. Therefore, the maximum baud rate on the data pair for the 4 Mbps operation is 8 Mbaud and the clock frequency is 8 MHz. An example of the encoding scheme for 4 Mbps operation is shown in Figure 82.

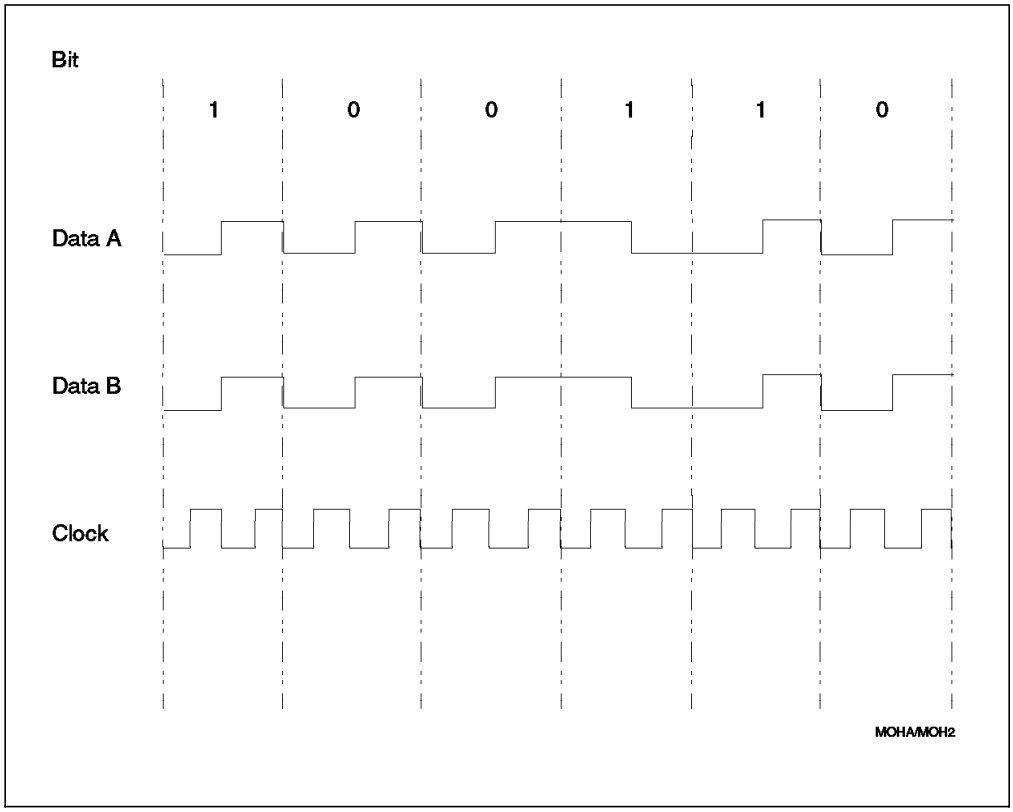


Figure 82. 8260 Backplane Signalling for 4 Mbps Operation

In 16 Mbps operation, using the same encoding technique as the 4 Mbps operation would result in a clock frequency of 32 MHz allowing little margin for timing or skew. Therefore, a different encoding scheme is used to reduce the baud rate and thus enhance the integrity of the signal on the 8260 backplane. For 16 Mbps operation, one of the data-signal shunt pairs (Data_A) carries the first half-bit of the Differential Manchester encoded data, while the other data signal (Data_B) carries the second half-bit and the clock signal, which is used to sample both data pairs. This encoding scheme results in a maximum data baud rate of 16 Mbaud and a clock rate of 16 MHz. An example of the encoding scheme used for 16 Mbps ring operation on the 8260 backplane is shown in Figure 83 on page 137.

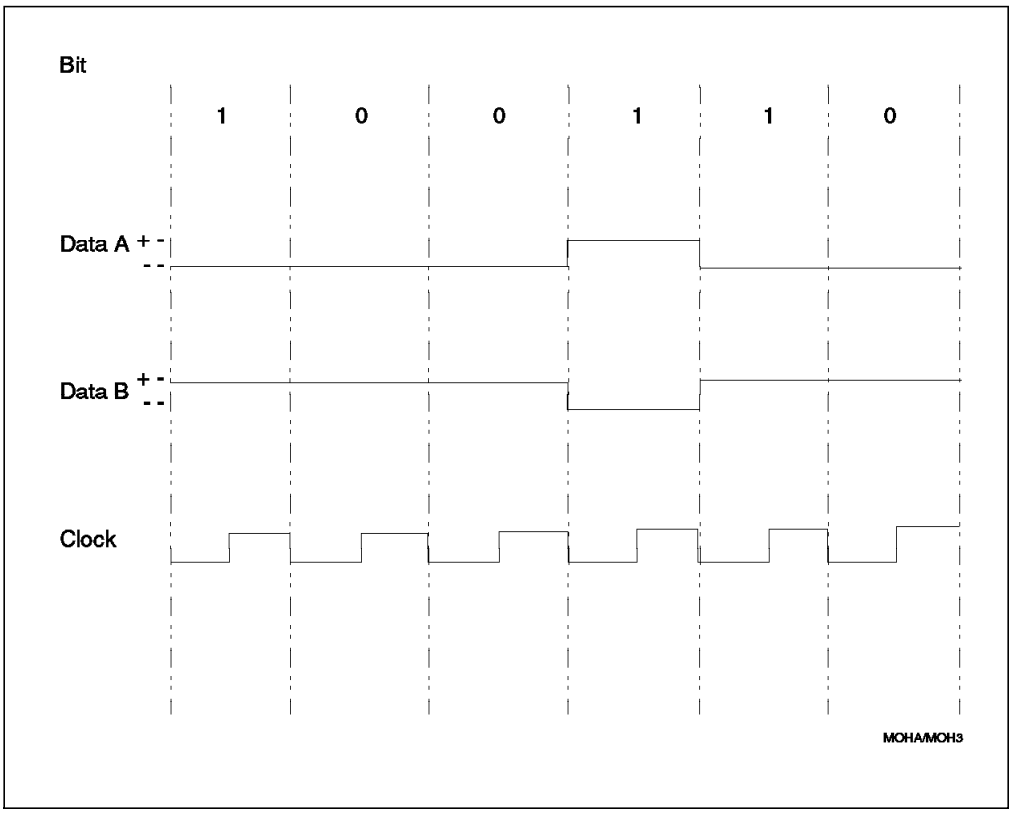


Figure 83. 8260 Backplane Signalling for 16 Mbps Operation

Note that the 8260 backplane interface is completely *digital*, whereas the signals sent on the transmission media (lobe cables and the cabling between two hubs) is said to be *analog*. In this context an analog signal is one where there is no separate clock signal. A digital signal is one where there are separate data and clock signals.

The use of digital signals on the 8260 backplane allows the signals to be switched to the appropriate location by using digital switches which can be easily implemented on the 8260 media modules. Per-port switching modules, where different ports on the same module may be assigned to different networks on the 8260 backplane, are made economically possible because of the digital signalling on the 8260 backplane.

Because of the use of digital signalling on the 8260 backplane, each 8260 media module must convert the analog signal it has received from the attached stations and convert it to a digital signal and then present the data and clock to the backplane. This is done within both the active and passive modules. In the opposite direction, the modules must receive the data and clock from the backplane and convert them to an analog signal before sending them on the transmission media for transmission to the stations.

The Phase Lock Loop (PLL) function which is implemented on each 8260 module, (DPLL is in 8.3, “Dual Phase Lock Loop” on page 138) is used to perform the conversion between the analog and digital signals. Also, in the 16 Mbps operation, the PLL will double the frequency of the received digital signals (clocked at 16 MHz) to form analog signals (clocked at 32 MHz) for transmission on the lobes, and does the opposite for the signals sent to the backplane from the lobe. In the 4 Mbps mode, the PLL does not change the frequency of the

signal as the signal is clocked at 8 MHz on both the backplane and the transmission media (lobe cables and inter-wiring closet cables).

8.3 Dual Phase Lock Loop

The intent of the dual PLL design of the 8260 is to isolate lobes from each other so the lobe length or type of cable will not affect what can be achieved on any other lobe of a ring segment. Below is a summary of the Dual PLL concept and its implementation in the 8260.

The current IBM token-ring adapters use a Phase Lock Loop (PLL) to derive a clock signal from the incoming data signal, and then use that clock to retransmit the data. As data is affected by crosstalk, noise, cable characteristics, etc. the phase of the transitions in the data shift around. This is referred to as jitter. Most of this jitter is filtered out by re-clocking the signal, but to the degree that the jitter affects the PLL, and therefore the clock output of the PLL, that jitter is passed on by the adapter. This jitter in the clock signal is passed on to the next station downstream. With each additional adapter, the amount of shift in the transitions grows. Eventually, the shift is large enough and fast enough that the next PLL cannot track with it, so the signal fails to be accurately retransmitted.

PLLs have a characteristic associated with them called *bandwidth*. The bandwidth determines how fast a change the PLL can track. The larger the bandwidth, the better the PLL can track the fast changing incoming signals, but higher bandwidths also mean more of the jitter is passed to the output, so just increasing the bandwidth does not result in more stations on a ring. What is needed is a PLL that behaves like a *wideband* PLL, but the clock output should behave like that from a PLL with a narrow bandwidth. That is what is implemented with the dual PLL concept.

A signal coming into an active port on an 8260 is first received by a PLL with a wideband characteristic. This bandwidth is set at approximately 400 kHz - similar to the PLL on the current IBM token-ring adapters. The clocked data from the wideband PLL receiver is then fed through a buffer, into a PLL circuit with a *narrowband* characteristic. As a comparison, the bandwidth of this PLL is set around 50 kHz. The buffer in between is required because at any point in time the wideband PLL may be clocking the incoming data at a different rate than the narrowband PLL is clocking data going out (because the wideband PLL shifts faster than the narrowband PLL). The result is a circuit that can receive a signal with a fair amount of jitter, but it retransmits a signal with a significant reduction in jitter.

As far as practical implementation, the 8260 puts a wideband PLL receiver on the incoming signal from each lobe, and puts the narrowband PLL in the transmitter of each lobe output. Figure 84 on page 139 shows the components of the DPLL as implemented in the 8260 media modules.

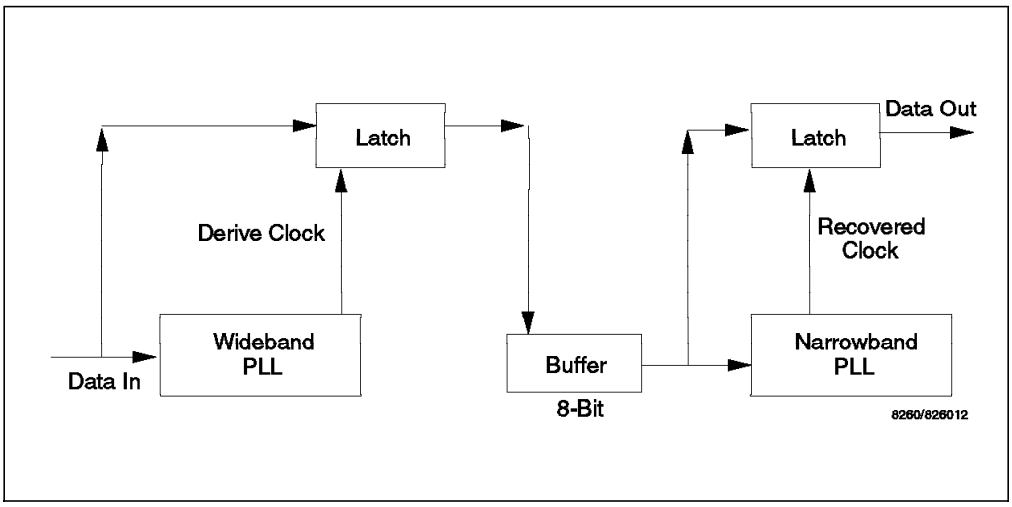


Figure 84. Components of Dual Phase Lock Loop

The reduction in the jitter would allow you to have longer lobe distances and higher number of station per ring segment. More details about the number of supported stations and the lobe cable length are provided in 8.6, “Active Port Technology” on page 142.

The DPLL is used in all the 8260 token-ring modules to ensure that the amount of jitter which enters the backplane has been minimized. This is the case with the passive modules as well as the active modules. However, active modules such as the 18-port active per-port switching module, 18-port active module switching module, and the dual-fiber repeater module implement one DPLL at every port, while the passive modules such as the 20-port passive module, implements just one DPLL at the interface to the backplane. The positioning of the two PLLs on each port of the active module is shown in Figure 85 on page 140.

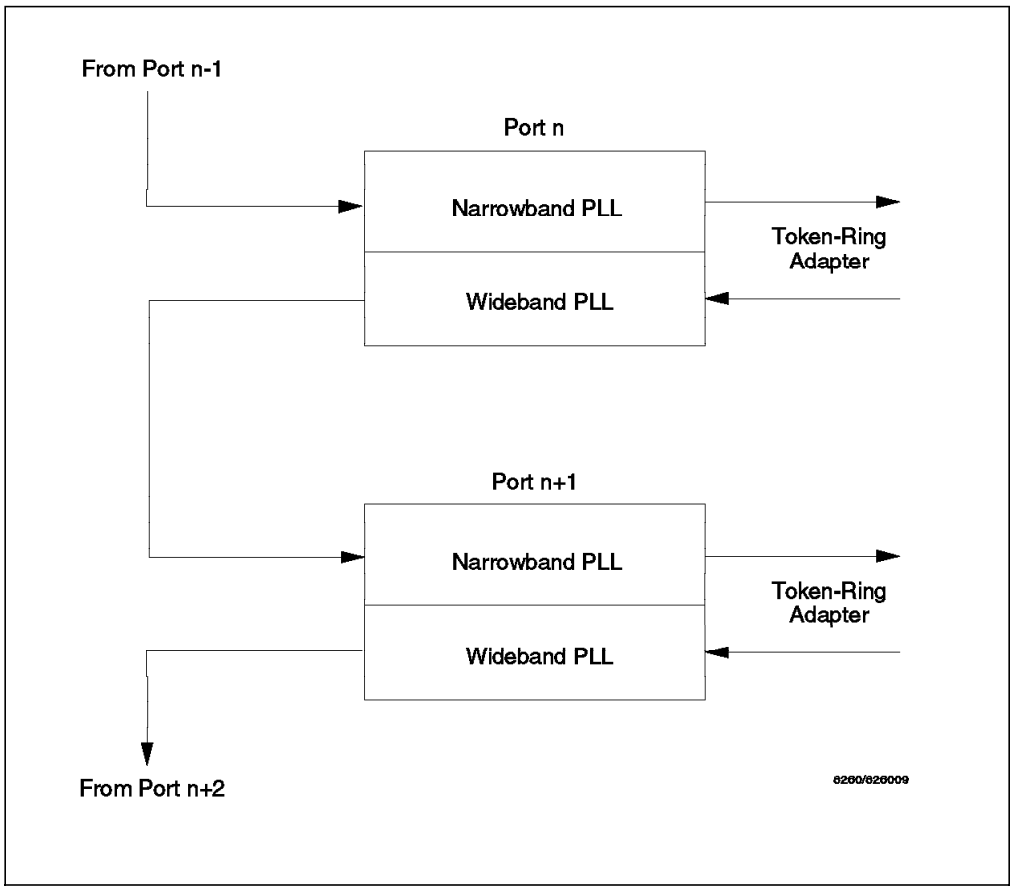


Figure 85. DPLL Implementation on Active Ports

Note

Since the jitter is removed from the signal before entering the backplane, the signal received from the backplane would only have a small amount of jitter accumulated on the backplane.

The signal received from the backplane goes through the narrowband PLL before being transmitted out of the port.

The passive module switching modules do not use DPLLs on each port. Instead, a Jitter Attenuation Daughter Card (JADC) is required which implements an enhanced DPLL function which can receive and eliminate a greater amount of accumulated jitter.

Note

Ports 17 and 18 on the 18-port active modules can be set up as either RI/RO or lobe ports using the jumpers provided on the module. When these ports are configured as RI/RO ports and your 8260 is connected via these ports to a non-8260 hub, a JADC **must** be installed on these modules to ensure that the jitter accumulated on the non-8260 hub, is reduced before it enters your 8260.

8.4 Jitter Attenuator Daughter Card (JADC)

The JADC can be mounted on any 8260 token-ring module and contains a DPLL function. It must be installed on a module under the following circumstances:

1. Your 18-port active module is configured with ports 17 and 18 acting as RI/RO ports and these ports are connected to a non-8260 hub.
2. The fiber ports on the dual-fiber repeater module are connected to a non-8260 hub.

   Note: The dual-fiber repeater module provides two sets of RI/RO pairs and you must install one JADC for each pair which is connected to a non-8260 hub. This module has the ability to accommodate two JADCs.
3. The 20-port passive module must always have a JADC. In fact, this module is shipped from the factory with the JADC already installed and must never be removed.

The DPLL on the Jitter Attenuator Daughter Card is similar to the DPLL implemented on each port of the 8260 active token-ring modules. The only difference is that the Jitter Attenuator Daughter Card has to cope with a higher amount of jitter which may be accumulated by up to 20 stations that may attach to the passive module or a high number of stations attached to the non-8260 hubs. The size of the buffer used in the Jitter Attenuator Daughter Card is 64-bits as opposed to the 8-bit buffer which is used in the DPLLs implemented on the active modules. Figure 86 shows the components of the DPLL implemented on the 8260 Jitter Attenuator Daughter Card.

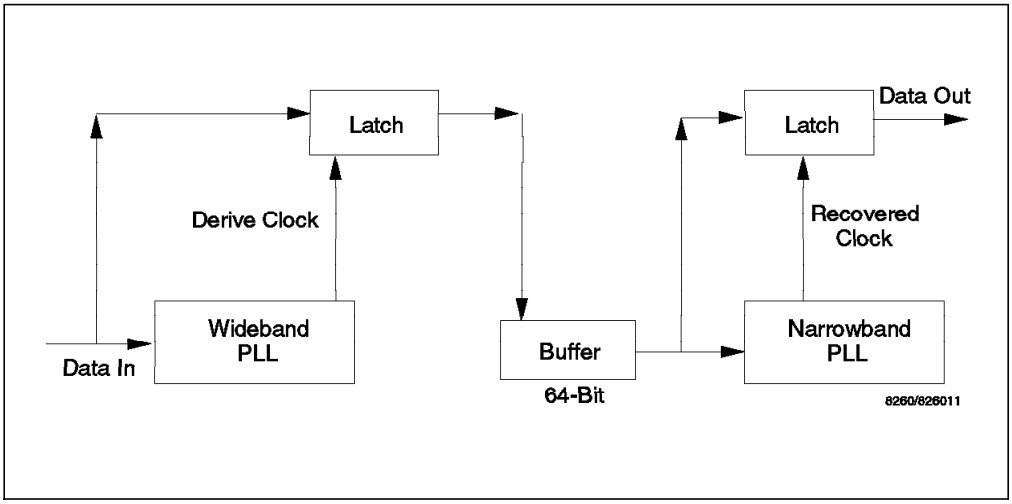


Figure 86. Components of DPLL Implemented on JADC

The DPLL of JADC on the passive module is located after the last port. The wideband PLL accepts signals from the last port, whereas the narrowband PLL takes the signal from the wideband PLL and transmits it out toward the backplane. In addition to the JADC, there is a DPLL module physically on the passive module whose narrowband side resides between the backplane and port 1, and its wideband side resides between the JADC and the backplane.

When a JADC is installed on an active module, the JADC is always positioned as a single unit (wideband and narrowband components) between the last trunk port and the backplane. In addition, the DPLL which is always present at each trunk port is changed from a narrowband/wideband configuration to a

wideband/wideband configuration when the port is in trunk mode. This is done to ensure that when the ring is reconfigured outside the module, a signal with a lot of accumulated jitter does not hit a wideband/narrowband configuration until it has gone through a JADC to remove the excessive jitter.

So, the following is a summary of the differences between the active and passive modules.

- A passive module has no active re-timing from port to port. The data is passed sequentially through the ports using relays to bypasses unused ports.
- The signal is re-timed and re-amplified for each port on the active modules. This allows longer lobes and a higher number of stations per ring segment.
- On the active modules, the DPLL on each port converts the analog signal from the external station to digital for transmission to the backplane. This means that the signal on the active modules are in digital form, making it economically possible to offer per-port switching on the active modules by using a switch fabric on the module that can switch the signals from each port to any one of the 10 backplane rings on the ShuntBus.

  Note: Currently, the Dual Fiber Repeater module and the 18-port per-port switching modules allow you to perform per-port switching.

8.5 Passive Port Technology

In the passive module implementation, the data is switched from port to port with no active re-timing or regenerative element between ports. This is done by a relay on each port. Data from attached workstations is passed from one port to the next without any re-timing and regeneration. Note that if a port is disabled or not used, the relay on that port will be wrapped to prevent the station on that port from entering the ring. This will result in the signal flowing to the active ports on each module.

On a passive module, as the signal moves from one port to another, jitter accumulated. Therefore, to pass the signal from the passive module to the backplane, we must remove the accumulated jitter and also convert the signal from analog to digital. In the opposite direction, we must convert the signal from digital to analog, before passing the signal from the backplane to the passive module.

8.6 Active Port Technology

In the active module implementation, each port contains a Dual Phase Lock Loop (DPLL) function. DPLL performs the following functions:

1. It removes the jitter received on each port before passing it to the next port on the module.

   The advantage of this function is that with the active modules, the maximum number of stations supported on a 4 and 16 Mbps ring is always 250 stations regardless of the type of cabling used. Also, you are allowed to mix UTP and STP cabling on the same module and/or the same ring segment of the 8260. For example, you can mix up to 250 stations connected to the 8260 active modules using STP and various types of UTP (category 3, 4 and 5) to form a single ring operating at 4 or 16 Mbps.

Note

Please note that it is incorrect to say that we support 250 stations at 4 Mbps. That is not necessarily true since there are some adapters on the market that implement the minimum elastic buffer required for each workstation adapter card. These cards, while not affected by the *rate of change* of accumulated jitter (which has always been the limitation on station count) are not able to accommodate the worst case total absolute jitter that can accumulate. Apart from the initial IBM 4 Mbps adapters which were offered by IBM about 10 years ago, there are no IBM adapters that implement the minimum buffer.

2. It regenerates the signal on each port. This function allows you to have longer lobe distances for UTP and STP than is permitted on the 8260 passive modules or other hubs that do not implement similar function. The maximum supported lobe length for the active modules is shown in Table 26.

Table 26. Lobe Distances Using 8260 Active TR Modules

Cable Type	4 Mbps Ring	16 Mbps Ring
STP	800	400
UTP Category 3	250	100
UTP Category 4	425	210
UTP Category 5	425	225
FTP	425	225

As a comparison, the maximum lobe length supported by the 8260 passive modules is shown in Table 27.

Table 27. Lobe Distances Using 8260 Passive TR Modules

Cable Type	4 Mbps Ring	16 Mbps Ring
STP	400	200
UTP Category 3	125	N/A
UTP Category 4	200	100
UTP Category 5	200	100
FTP	425	225

3. The signal received from each lobe is converted to a digital form before entering the module. The digital signal on the active modules makes it easy to manipulate the flow of data on a per-port basis allowing IBM to offer active per-port switching modules.

8.6.1 Per-Port Switching on the Active Modules

Currently, IBM offers the following active per-port switching modules:

- 18-port active per-port switching module
- Dual fiber repeater module

In these active per-port switching modules a switch fabric is employed so that every port has a possible transmission path to every other port and the 10

backplane rings on the ShuntBus. This enables you to form multiple rings on a single module using this switch fabric. This is shown in Figure 87 on page 144.

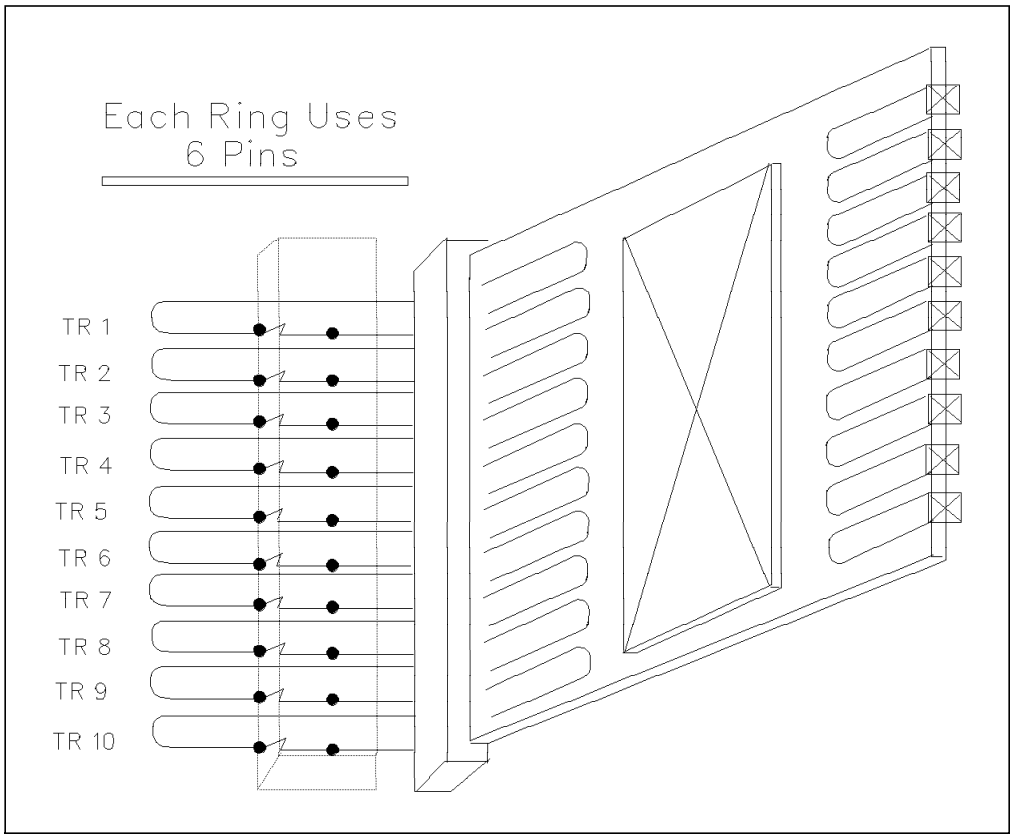


Figure 87. Token-Ring Per-Port Switching

The rings to which the various ports on a per-port switching module can attach may be a mixture of 4 and/or 16 Mbps segments. Therefore, a single active module can be used to accommodate stations operating at different speeds. Also, the multiple rings on a single active module can be a mixture of the 10 backplane segments on the ShuntBus (token_ring_1 thru token_ring_10) and the 11 isolated segments (isolated_1 thru isolated_11) which exist on each active module.

The isolated segments on the active modules can be used to set up token-ring segments between two or more stations on that module, without using the backplane. Also, note that each isolated segment on a single module can be configured to operate at 4 or 16 Mbps.

Note

With the 18-port active per-port switching module the lobe ports can be distributed concurrently across a total of 11 segments which can be a mixture of backplane token-ring segments and isolated segments on the module. However, on the same per-port switching module you cannot allocate an isolated segment number which matches the number of a backplane segment to which other ports on the module are attached. For example, you cannot assign any ports to isolated_1 if you already have ports assigned to token-ring_1. The consequence of this limitation is that, the total number of segments to which the ports on the active modules can be attached to is 11 segments.

Also, since by default the module ships with ports switched to backplane token-ring_1, you cannot have an isolated_1 allocated on the module unless you detach the ports from token-ring_1.

One general tip which you might follow is that when assigning ports to backplane and isolated segments you start numbering the backplane segments from 1 upwards and the isolated segments from 11 downwards.

8.6.2 Static Switch on the Per-Port Switching Modules

Each 8260 active per-port switching module implements a *static switch* for each of its port. The static switch may be used as a safeguard against switching an open adapter from one ring to another.

To understand the reasons for the static switch, let's review the functions which are performed by each station when it first attaches to a token-ring. The following is a summary of these functions:

1. Lobe test

   The station sends a series of Lobe Test MAC frames on the lobe to make sure that the lobe is not faulty.

2. Insert into the ring

   The station applies the phantom signal and enters the ring.

3. Check for active monitor

   After entering the ring, the station checks to see if an active monitor station is present on the ring by listening for Active Monitor Present, Standby Monitor Present or Ring Purge MAC frames. If any of these types of frame are seen within a time frame called "T(attach)" timer, it is assumed that there is an active monitor present on the ring and the station will assume the role of a standby monitor. However, if the "T(attach)" timer expires and none of the above frame types are seen, the station assumes that either it is the first station on the ring or there is no active monitor; it will then initiate the "token-claiming" process.

   Note: Token-claiming process is used to elect an active monitor on the ring.

4. Duplicate address test

   The station checks for the presence of another station with the same address on the ring using the Duplicate Address Test MAC frame. If a duplicate address is found, the station removes itself from the ring.

5. Participation in neighbor notification

   By participating in the neighbor notification, the station learns the address of its Nearest Active Upstream Neighbor (NAUN). It also identifies itself to nearest active downstream neighbor.

6. Request initialization

   The station issues a Request Initialization MAC frame which will be sent to the Ring Parameter Server (RPS) functional address. This frame is used to request operational parameters such as the ″ring segment number″ and ″Soft Error Timer Value″ from the Ring Parameter Server if one present. The Ring Parameter Server will provide this information to the station by transmitting an Initialize Ring Station MAC frame.

   The Request Initialization MAC frame is also used to register the station with the LAN Network Manager if one is present on the network.

In a per-port switching module, if you switch a port from one ring to another, while the adapter is open, the station will not perform some of these functions such as testing for duplicate MAC address. It is, therefore, conceivable that if the administrator is not careful, an open adapter can be moved to another ring which contains an adapter with the same address. This will result in having two stations on the same ring which can produce unpredictable results.

To prevent a station from being able to be switched from one network to another, the static switch can be set to *enabled*. In that case, you can only switch the port if the phantom voltage on that port is dropped. In other words, when the static switch is enabled, you can not switch an open adapter from one ring to another.

You can display the status of the static switch for each port by using the following DMM command:

```
SHOW PORT {slot.port} VERBOSE
```

An example of the output from this command is shown in Figure 88.

```
8260> show port 6.1 verbose


Port Display for Module T18PSA :

Port  Mode     Status              Network          General Information
----- -------- ------------------- ---------------- --------------------
06.01 ENABLED  OKAY                TOKEN_RING_10

Alert Filter:                           DISABLED
Port Connector:                         RJ45S
Dip Network Setting:                    TOKEN_RING_1
Static Switch:                          DISABLED


8260>
```

Figure 88. Static Switch Display for Active Per-Port Switching Ports

You can modify the status of the static switch for each port using the following DMM command:

```
SET PORT {slot.port} STATIC_SWITCH {enable|disable}
```

If you try to switch a port with *enabled* static switch from one segment to another, you will get the an error message. This is shown in Figure 89.

```
8260> set port 6.1 static_switch enable
Port 06.01 static switch set to ENABLED.
8260>
8260> show port 6.1 verbose


Port Display for Module T18PSA :

Port  Mode     Status              Network          General Information
----- -------- ------------------- ---------------- --------------------
06.01 ENABLED  OKAY                TOKEN_RING_10

Alert Filter:                           DISABLED
Port Connector:                         RJ45S
Dip Network Setting:                    TOKEN_RING_1
Static Switch:                          ENABLED


8260> set port 6.1 network token_ring_1
Port 06.01 static switch enabled and phantom present: command aborted.

8260>
```

Figure 89. Switching Ports with Enabled Static Switch

Also, note that apart from the possible problem discussed above, there are some other situations that may cause a problem when you switch an open adapter from one network to another. For example, in Figure 90 on page 148, station ″A″ is attached to ″ring 1″ and is communicating with the SNA host via the 3745 attached to ″ring FFF″. As the path between station ″A″ and the host involves a source routing bridge (bridge 1), the Routing Information field used in the frames between station ″A″ and the host contains ring ″1″, bridge ″1 and ring ″FFF″. Now, if in the middle of your SNA session, you switch station A to ″ring 2″, the actual path between station ″A″ and the host will change, while station A and the host still use the old Routing Information field. This will result in the frames sent by station ″A″ not being delivered to the host and vice versa, the frames sent by the host will not be delivered to station ″A″. The result of this is that your stations will lose contact and the SNA session will be terminated after your SNA timeout period. Of course, after the session termination, station ″A″ can try to contact the host using the route discovery in source routing. This will result in the new route (ring ″2″, bridge ″2″, ring ″FFF″) being discovered and a new session being established. So, in this case the switching of the port from one segment to another, results in the termination and re-establishment of existing sessions.

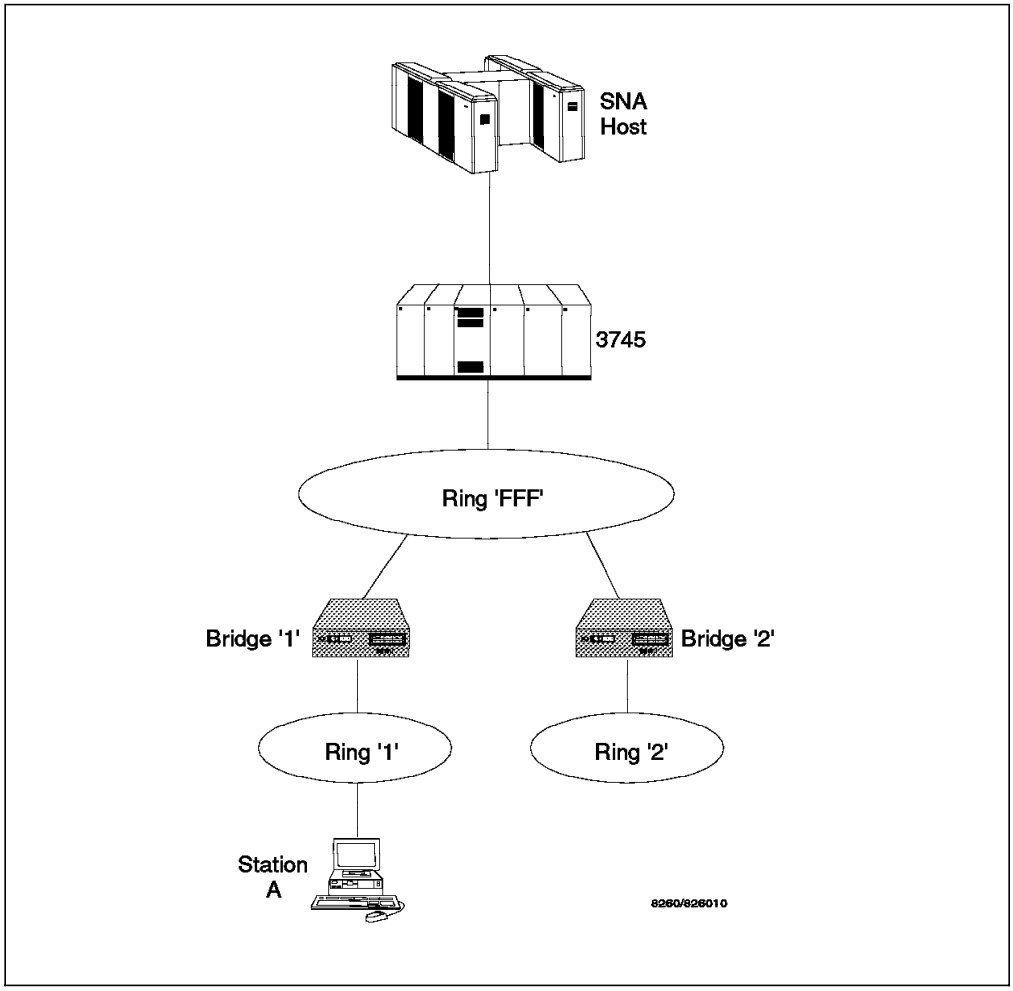


Figure 90. Port Switching with Source Routing Bridges

8.7 Signal Flow on the 8260 Token-Ring Modules

On the module switching modules (active or passive), the signal flow is predefined on the module basis. That is, the signal which is received from the backplane is always passed to the first active port, then to the next active port, and finally from the last active port to the backplane. Of course, if the module is isolated, the backplane is not involved; instead the signal flows from the last active port back to the first active port. Therefore, in the module switching modules, the ordering of the stations on the ring is dependent on the physical placement of the stations on the module (the station on port 1 is upstream of the station on port 2, etc.). If the ring consists of more than one module, the ordering of the stations on the ring also depends on the physical placement of the modules in the concentrator (the module in slot 1 is upstream of the module in slot 2, etc.).

In the active per-port switching modules, the same principle as the module switching modules apply; that is, the module in the lower-numbered slot is upstream of the module in the higher-numbered slot and within a module the lower-numbered port is upstream of the higher-numbered port. However, you must bear in mind that different ports on the same per-port switching module may be assigned to different networks (backplane or isolated segments).

8.8 Speed Detection

Speed detection on the 8260 token-ring media modules is achieved in one of two ways depending on the module type.

8.8.1 Speed Detection on Active Modules

For the active modules, speed detection is accomplished by counting the number of transitions in the incoming data over a set period of time. If the rate of transition is less than 4.5 MHz the station would only be allowed to enter 4 Mbps token-rings and if the rate of transition is more than 4.5 MHz, the station would only be allowed to enter 16 Mbps token-rings. So, if the module detects that the station is trying to insert at the wrong speed, the speed mismatch will be detected and the station will be prevented from inserting into the ring and disrupting its operation.

When an incorrect speed is detected, the port is not allowed to unwrap (note that under normal circumstances, when the station enters the ring, the port is in wrapped state) and the status of the port is set to ″speed mismatch″. The port will then be checked again when a transition of phantom is detected or when the user disables and then enables the port.

Note

During the configuration of the 8260, you will set the ring speed for the networks (token-ring-1 thru token-ring-10 and isolated_1 thru isolated_11) using the following DMM command:

```
SET NETWORK TOKEN_RING token_ring_n RING_SPEED {4mbps|16mbps}

SET NETWORK TOKEN_RING isolated_n {slot} RING_SPEED {4mbps|16mbps}
```

Once, you set the ring speed, any port attached to that ring will assume the speed of the ring. You do not set the ring-speed for each port.

8.8.2 Speed Detection on Passive Modules

Passive modules implement a software-based method to detect incorrect ring speed on the attaching stations.

When a station inserts into the ring on a passive module, the module will first wrap all the other ports on the module and also the module off the backplane. Then, the Recovery ASIC in the module sends an All-Station MAC frame (at the speed of the ring to which this port is assigned) on the newly inserted port. The ASIC will wait for this MAC frame to be returned and it will inspect the ″A″ (address-recognized) and ″C″ (frame-copied) bits on the received frame.

- If the ″A″ and ″C″ bits are set to B′1′ the station which just inserted into the ring is operating at the correct speed. The Recovery ASIC will then allow the station to insert into the ring and will also unwrap all the other ports on the module allowing the existing users to resume access to the ring. During this process, the existing stations on the module are unable to access the ring. However, since this is a very short time, no user sessions are expected to be terminated as a result of this temporary inability to access the ring.

- If the ″A″ and ″C″ bits are not set to B′1′, the port which just inserted into the ring is assumed to be operating at the wrong speed. The Recovery ASIC will prevent that port from entering the ring and will also unwrap all the wrapped ports allowing the existing stations to resume their access to the ring.

When an incorrect speed is detected on the inserting station, the port is wrapped and the status of the port is set to ″speed mismatch″. The port will only be unwrapped when a transition of phantom is detected on that port or when the user disables and then enables the port.

A threshold for speed detection can be set for each passive module using the following DMM command:

```
SET MODULE {slot.subslot} SPEED_THRESHOLD {0 to 255}
```

This threshold is the number of times that the port will be unwrapped as a result of the phantom signal transitions. When the threshold is exceeded, the port will remain wrapped with a status of ″SPD THRES EXCEEDED″ until the user disables and re-enables the port. The counter for this threshold is reset every time a port successfully inserts into the ring.

Note that the process of speed detection on the passive modules prevents the existing stations from accessing the ring for the duration of the speed detection process. Therefore, the use of this process is provided as a configuration option on the passive modules. Users can enable or disable the speed detection on each port of a passive module, using the following DMM command:

```
SET PORT {slot.port} SPEED_DETECT {enable/disable}
```

Note

The passive modules are shipped from factory with speed detection turned off for all the ports.

The current settings of the SPEED_DETECT function for each port can be displayed using the following command:

```
SHOW PORT {slot.port} VERBOSE
```

An example of the output from this command is shown in Figure 91.

```
8260> show port 5.1 verbose


Port Display for Module T20MS :

Port  Mode     Status              Network          General Information
----- -------- ------------------- ---------------- --------------------
05.01 ENABLED  NO PHANTOM          TOKEN_RING_10    Port is down

Alert Filter:                           DISABLED
Port Connector:                         RJ45S
Speed Detection:                        ENABLED
Speed Detection Dip Setting:            DISABLED

8260>
```

Figure 91. Port Display for Token-Ring Passive Ports

8.9 Beacon Recovery

8.9.1 Introduction

When a station detects a failure of token-claiming following a hard error, it transmits Beacon MAC frames with an all-station address to its ring, pacing them at a specified time interval known as ″T(transmit_pacing)″. This process will continue until the input signal is restored, or until this station removes itself from the ring for self-testing, as described below.

The issued Beacon MAC frames contain the issuing station′s source address, its NAUN (Nearest Active Upstream Neighbor) address as well as the type of the error detected. By inspecting these Beacon frames, the *beacon domain* (the two stations between which lies the cause of beacon) can be determined.

When the beaconing station′s NAUN has copied eight of these Beacon MAC frames, the NAUN station removes itself from the ring and tests itself and its lobe (using Lobe Media Test and Duplicate Address Test MAC frames). If the test fails, the NAUN remains out of the ring allowing the normal operation of the ring to resume. If the test is successful, the NAUN re-enters the ring.

If the ring does not recover after a specified period of time known as ″T(beacon-transmit)″ the beaconing station assumes its NAUN has completed its self-test and did not find any fault and has re-entered the ring. Therefore, the beaconing station removes itself from the ring and tests itself and its lobe using the same procedure as its NAUN. If the test fails, the beaconing station remains out of the ring, resulting in the signal being restored to the ring and the normal operation of the ring being resumed. If the test is successful, the beaconing station re-enters the ring and continues to send the Beacon MAC frames.

If the ring does not recover after both the beaconing stations and its NAUN have been tested, the error cannot be repaired by the attaching stations, and some other function must intervene to resolve the problem. In the 8250, this function is performed by the Token-Ring Management Module (TRMM), whereas in the 8260, the beacon recovery is performed by the media modules.

8.9.2 Beacon Recovery in the 8250

The TRMM can detect beaconing conditions on the ring to which it is attached through its token-ring MAC chip. The TRMM will use the following resources to attempt to find the cause of the beaconing and disable a port or trunk or isolate a module:

- The token-ring map indicating MAC addresses and their corresponding port. This map is built and maintained by the TRMM.

  By listening to the neighbor notification process (one complete sequence of Active/Standby Monitor Present MAC frames), TRMM can determine the MAC addresses of all the stations that are attached to the ring. Then, by using its own MAC address and also the knowledge that it has of all the ports which are active (a phantom signal detected) in the hub managed by this TRMM, it determines which of these MAC addresses are connected to the hub which is managed by this TRMM and which MAC addresses are external (connected to other hubs or are on a backplane ring other than the one to which this TRMM is attached). The other hubs, can be 8228, 8230, 8250, 8260 and/or OEM hubs.

To ensure that TRMM has an accurate ring map, you must issue the following command for each port that has a MAC-less station (such as token-ring tracing tools) attached to it:

```
SET PORT {slot.port} STATION_TYPE mac_not_present
```

8250 token-ring modules are shipped from the factory, with ″mac_present″ as default, which must be used for normal stations.

You also need to issue the following command for each copper trunk port to ensure the correct port-to-address mapping:

```
SET TRUNK {slot} RING_IN.{trunk port} NETWORK_MAP {external|internal}
```

In the above command you must specify *external* when the copper trunk port is used to connect to a module on a different hub, and you must specify *internal* when the copper trunk port is used to connect to a module on the same hub.

- The Beacon packet. The Beacon packet contains the source of the beaconing and its Nearest Active Upstream Neighbor (NAUN). The NAUN is the destination address of this packet.
- Information from the media modules indicating ports and trunks which have just been enabled.
- User setup indicating which ports have MAC-less stations (that is do not participate in ring poll process).
- User setup indicating the status of the external_beacon_recovery attribute on the trunks.

  With TRMM V3.0 the operator can issue the following commands for the trunks:

  ```
  SET TRUNK {slot} RING_IN.n EXTERNAL_BEACON_RECOVERY {exists|non_exists}
  or
  SET TRUNK {slot} RING_IN EXTERNAL_BEACON_RECOVERY {exists|non_exists}
  ```

  The effects of issuing this command for a trunk are discussed later in this section.

When beaconing is detected, the TRMM waits for up to 3 seconds to verify beaconing is still active. The TRMM will then attempt to use the last current logical map of the concentrator to determine the cause of the beaconing. Depending on the reaction of other adapters to the beaconing condition (that is, some adapters will be removed to test the beaconing condition) the map may not EXACTLY represent the state of all ports at the exact time of beaconing. This is why different steps of the algorithm are performed to attempt to find the beaconing condition even if the map has changed.

The following steps will be taken to try to determine the cause of beaconing. After each step, the algorithm will wait up to 10 seconds to verify that beaconing is gone to see if an action worked. The 10 second delay is necessary to prevent errors due to the cause of the beaconing removing itself to test its lobe port connections at the same time an action is taken. This could erroneously cause a port/trunk to be disabled which was not the source of the problem. If the action did not fix the beaconing the TRMM will undo the action (that is, re-enable port if it was disabled) and go to the next step.

1. Shut down the most likely cause of beaconing - new trunk connections * or newly enabled ports (″new″ indicating TRMM has not seen a valid MAC address after a port or trunk was enabled).

2. Isolate any new modules that have logical ports on the ring (logical is a port which cannot be disabled such as TRMM or bridge).
3. If the source or destination address in the packet is external to the hub, wait for up to 5 seconds to check if the beaconing can be disabled externally.
4. If the source or destination address in the packet is external to the hub, disable all external trunks.
5. Disable any enabled ports on fiber repeater (these ports may show as external if both sets of trunks on the fiber repeater are enabled).
6. Disable any enabled ports that are between the source and destination addresses contained in the beaconing packet.
7. Isolate any modules that are between the source and destination addresses contained in the beaconing packet.
8. If both addresses are internal to the hub and there are enabled trunks in between, disable the trunks.
9. Disable port corresponding to destination address.
10. If the destination in beaconing packet is external, shut down all external trunks *.
11. Disable the port corresponding to the source address.
12. If the source of beaconing packet is external, shut down all external trunks *.
13. If any MAC-less devices are present on the ring, disable the ports corresponding to these devices.
14. Disable external trunks again to test for condition where beaconing was fixed temporarily externally *.
15. Isolate modules one at a time until beaconing is detected to be gone. If beaconing goes away put module back on network and disable ports on that module until beaconing goes away. When beaconing ends, the correct port has been found.
16. Isolate the TRMM if all else fails.

* When external trunks are disabled and the disabling fixes the beaconing problem perform the following:

- Re-enable all trunks with external beacon recovery non_exists.
- If no beaconing, re-enable trunks with external beacon recovery exists.
- If beaconing now detected, shut down all trunks with external beacon recovery exists. Re-enable trunks one at a time until source of beaconing is detected and then disable that trunk.
- If beaconing when trunks with external beacon recovery non_exists are re-enabled, then disable all these trunks. Re-enable trunks with external beacon recovery exists.

In case the NAUN of the station issuing Beacon MAC frame is the TRMM itself, the TRMM will take itself off the ring to perform the self-test as any other station. If there is no problem with TRMM, it re-enters the ring. However, if a problem is found in TRMM, it will stay off the ring and isolated. In this case the beacon problem is resolved, but the ring is now operating without TRMM and if another station causes a beacon condition that requires TRMM intervention the operation of the ring will be disrupted.

TRMM V3.0 allows you to enable/disable the beacon recovery function using the following command:

```
SET DEVICE BEACON_RECOVERY {enable|disable}
```

Note that this feature must be enabled during normal operation; however, you may disable this feature as a trouble shooting tool, to prevent the ring from recovering before the faulty device is isolated.

TRMM V3.1 allows you to change the ″beacon timeout″ (the amount of time that the TRMM will wait before attempting to unwrap the RI/RO ports after these ports are wrapped due to a beacon condition) using the following TRMM command:

```
SET DEVICE BEACON_TIMEOUT {number of second}
```

The allowed range for this command is 1 to 100 seconds.

You can display the status of the TRMM ″beacon_recovery″ and ″beacon_timeout″ using the following TRMM command:

```
SHOW DEVICE
```

An example of the output for this command is shown in Figure 92.

```
8250> show device
TO1MS Token Ring Management Module (Advanced-MGT) v3.10-A pSOS+ SNMP
Name:   8250
Location:
ITSO LAB, Raleigh
For assistance contact:

Mohammad Shabani X2339
Boot EPROM Version:  v3.00-A    Size:  256 KBytes
Flash EPROM Version: v3.10-A    Size: 1024 KBytes  DRAM Size: 2048 KByte
Serial Number: 1088813          Restarts: 6     Service Date:  94/09/06

Interface  IP Address       Subnet Mask   Primary Gateway  Secondary Gat
---------  ---------------  -----------   ---------------  -------------
    1 *    009.067.046.235  FF.FF.FF.F0   009.067.046.238*  000.000.000.
    2      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    3      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    4      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    5      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    6      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    7      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
    8      009.067.046.235  FF.FF.FF.F0   009.067.046.238   000.000.000.
MAC Address: 10-00-F1-0F-30-B7
Dip Configuration:  DISABLED    Diagnostics:     ENABLED
Trap Receive:       DISABLED    Beacon Recovery: ENABLED
Monitor Contention: ENABLED     Beacon Timeout:  10 second(s)
8250>
```

Figure 92. Show Device Command for TRMM

8.9.3 Beacon Recovery in the 8260

Beacon recovery in the 8260 has been improved by distributing the beacon recovery process to each of the 8260 token-ring media modules (both active and passive). This allows you to manage an 8260 consisting of multiple token-ring segments using a single DMM and protect multiple rings from beacon problems without the need to have one DMM for each segment.

Each 8260 token-ring media module has a built-in chip called Recovery ASIC (Application Specific Integrated Circuit) which provides beacon recovery for the stations attached to that media module.

8.9.3.1 Recovery ASIC

The recovery ASIC has two entities. These two entities are called ″Upstream Recovery ASIC″ or URA and ″Downstream Recovery ASIC″ or DRA. Both entities have a burnt-in MAC address. These MAC addresses are only used for beacon recovery and do not limit the maximum number of MAC addresses on a ring.

In the case of module switching modules, the Recovery ASIC is always attached to the ring configured for that module and the URA is located between the backplane and the first port of the module while DRA is located between the backplane and the last port of that module. This is shown in Figure 93.

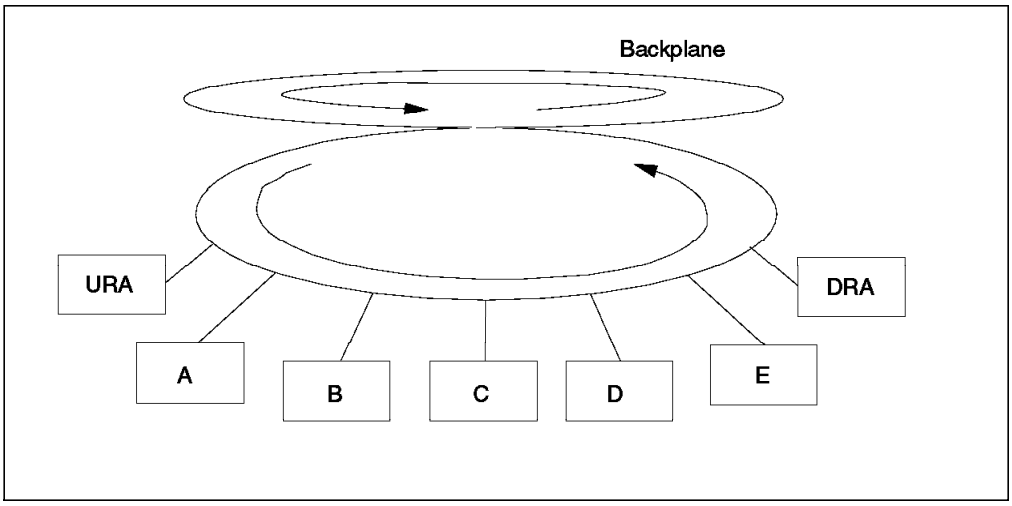


Figure 93. Recovery ASIC in Module Switching Module

In the case of per-port switching modules, as the ports on the module can be attached to multiple backplane segments, the Recovery ASIC is not connected to any of the backplane rings under normal operating conditions. Instead, associated with each port is a function called Ring Monitor (see 8.9.3.2, “Ring Monitor on the Per-Port Switching Module” on page 157 for details) which is placed upstream of its associated port and monitors for beaconing condition. As soon as a beacon condition is detected on one of the rings to which this module′s ports are attached, then the Recovery ASIC will be inserted into that ring to provide the beacon recovery function. In this case, the DRA will be placed between the backplane and the last port of this module on the beaconing ring. Also, the URA will be inserted into the backup path if ports 17 and 18 are configured as trunk ports. This is shown in Figure 94 on page 156.

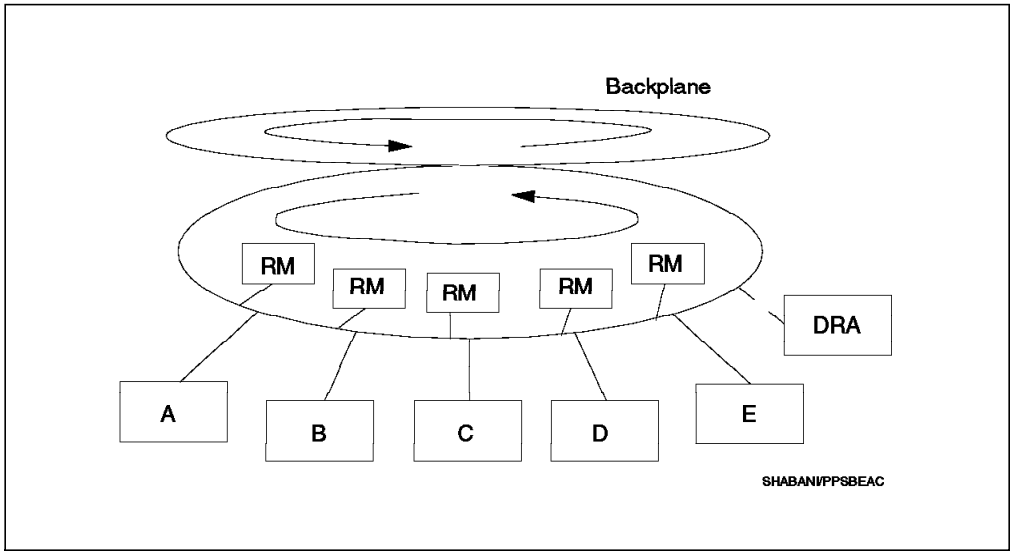


Figure 94. Recovery ASIC in Per-Port Switching Module

You can find out the MAC address of the Recovery ASIC on each module by using the following DMM command:

```
SH MODULE {slot.subslot} VERBOSE
```

Figure 95 showsDisplay the output from this command for a 20-port passive token-ring module.

```
8260> show module 5.1 verbose

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
05.01 T20MS           v1.00   TOKEN_RING_10 Port(s) are down

T20MS: Token Ring Passive Module Switching Twisted Pair

Boot Version:                             v1.00
Ring Speed Dip Setting:                   16 MBPS
Dip Network Setting:                      TOKEN_RING_1
Non-Volatile DIP Setting:                 ENABLED
Recovery Asic Primary Address:            08-00-8f-d0-38-43
Recovery Asic Secondary Address:          08-00-8f-d0-38-83
Beacon Threshold:                         255
Speed Detect Threshold:                   15


8260>
```

Figure 95. Display Output for 20-Port Passive Module

Figure 96 on page 157 shows the output from this command for an active 18-port per-port switching token-ring module.

```
8260> show module 6.1 verbose

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
06.01 T18PSA          v1.00   PER_PORT      Trunk(s) are down

T18PSA: Token Ring Active Port Switching Twisted Pair Module

Boot Version:                             v1.00
Ring Speed Dip Setting:                   16 MBPS
Jitter Attenuator 1 Status:               OKAY
Non-Volatile DIP Setting:                 ENABLED
Recovery Asic Primary Address:            08-00-8f-d0-e0-e2
Recovery Asic Secondary Address:          08-00-8f-d0-e0-62
Beacon Threshold:                         7
Switch ASIC type:                         BASIC


8260>
```

Figure 96. Display Output for 18-Port Active Per-Port Switching Module

To perform beacon recovery, the Recovery ASIC operates in one of the following three modes:

1. MAC frame monitor:

   In this mode the recovery ASIC is listening for Beacon MAC frames. This is the normal mode of operation for the Recovery ASIC.

2. Frame transmit:

   In this mode the recovery ASIC can transmit Beacon Type 1 MAC frames. The Recovery ASIC enters this mode when it sees a Beacon Type 2, 3 or 4 MAC frame.

   Note: A Beacon Type 1 MAC frame is used for management purposes. Beacon MAC frames from a normal ring station are type 2, 3 or 4 depending upon the fault.

3. Manual mode:

   This mode is used for ring reconfiguration with 8250 repeaters and using proprietary 8250 trunk unwrapping.

Before describing the procedure used by the Recovery ASIC, to recover the beaconing conditions, let′s review the ring monitor function which is implemented on the per-port switching modules.

8.9.3.2 Ring Monitor on the Per-Port Switching Module

Ring monitor is a function which is employed on each port of the active per-port switching module and the dual-fiber repeater module and is required to assist the Recovery ASIC to perform beacon recovery on these modules.

Ring monitors have the responsibility to monitor their respective port for the following:

- The presence of a Beacon MAC frame
- The presence of AMP/SMP (Active Monitor Present/Standby Monitor Present)
- Tokens

Ring monitors are associated with each port and can be switched from upstream to downstream of that port. When the ring monitor detects a Beacon MAC frame on the ring, it calls in the Recovery ASIC to perform beacon recovery and isolate the faulty port (station). The following sections describe the beacon recovery procedures employed in the module switching modules and the per-port switching modules.

8.9.4 Beacon Recovery on the Module Switching Modules

As described in 8.9.1, “Introduction” on page 151, when a ring station detects a failure of token-claiming following a hard error, it transmits a Beacon MAC frame. The Beacon MAC frame can be one of the following types:

- Type 2
- Type 3
- Type 4

The Downstream Recovery ASIC (DRA) is normally operating in ″MAC frame monitor″ mode, but as soon as it detects one of the above beacon frames, it enters ″frame transmit″ mode and starts transmitting Beacon Type 1 MAC frames.

Note

If DRA sees a Beacon Type 1 (that is, a Beacon MAC frame issued by a DRA on another module) it will remain in ″MAC frame monitor″ mode and will not issue its own Beacon Type 1 MAC frames. This happens when a beaconing condition is encountered on another module which is attached to the same ring as this module.

The Beacon Type 1 MAC frames issued by DRA will first go onto the backplane and then through all the other token-ring modules and lobes that make up the beaconing ring. If the Beacon frames reach the Upstream Recovery ASIC (URA) on this module, two conclusions can be made:

1. The rest of the ring is complete and operating normally and
2. The fault must be somewhere in this module or the stations attached to this module or on the trunks

At this point, the module is wrapped from the backplane and Recovery ASIC begins wrapping ports sequentially, starting with the first active port upstream of DRA. The wrapping of the ports continues until the normal operation of the ring is restored. The normal operation of the ring is detected when the DRA starts receiving its own Beacon Type 1 MAC frames. At this point, the Recovery ASIC, has isolated the beacon fault domain to two ports (the last two ports which are wrapped) on this module.

To determine which one of the two ports is causing the beaconing condition, it now wraps all the ports on the module and then tests each of the two ports in the fault domain individually. The faulty port will be wrapped permanently and the remaining ports of the module will be unwrapped and the module will be inserted back into the backplane ring.

For example, in Figure 97 on page 159, if a beaconing condition is caused by station ″B″ attached to module 1, the downstream station (station ″C″), will

detect this and will issue Beacon MAC frames. These Beacon MAC frames will be repeated by each station (station ″D″ in this case) until they arrive in the DRA in module 1. Upon seeing these Beacon MAC frames, the URA on module 1 will issue Beacon Type 1 MAC frames. The Beacon Type 1 MAC frames will be repeated by every station on module 2 (including the URA and DRA on module 2) until they arrive in the URA in module 1. At this point, the Recovery ASIC on module 1 concludes that the rest of the ring (that is module 2 and its attached stations as well as the backplane) is operational, therefore, the beaconing condition must be on this module.

Recovery ASIC on module 1 starts taking recovery action by isolating module 1 from the backplane and deactivating its ports starting with the one upstream of its DRA (station ″D″) and checking for the status of the ring. After the port attaching station ″D″, the port attaching station ″C″ will be deactivated and so on. As soon as it deactivates the port attaching station ″B″, the beacon condition is removed; therefore, the fault domain is between station ″B″ and station ″C″. The Recovery ASIC will then deactivate all the ports on module 1 and then check station ″B″ and station ″C″ individually, and when it finds that station ″B″ is the source of problem, it deactivates the port attaching station ″B″ permanently and then reactivates all the other ports and inserts the module back into the backplane.

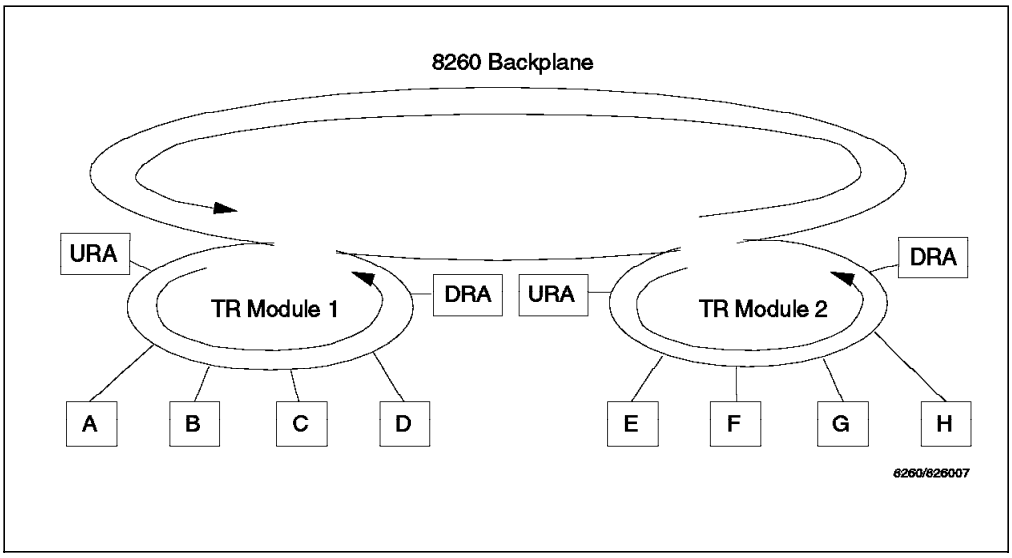


Figure 97. Beacon Recovery on the Module Switching Modules

8.9.5 Beacon Recovery on the Per-port Switching Modules

The per-port switching module might have stations attached to 11 token-ring segments consisting of the 10 different rings on the backplane and 11 isolated rings on the module. Therefore, the Recovery ASIC (of which we have only one on each module) is not connected to any rings under normal operating conditions. Instead, the Ring Monitor function (which is implemented on each port) is used to assist the Recovery ASIC with the beacon recovery process in the per-port switching modules.

Under normal operating conditions, the Ring Monitor is located upstream of its associated port. When a Ring Monitor detects the presence of a beaconing condition, by noticing Beacon MAC frames, it alerts the Recovery ASIC. The Recovery ASIC will then be inserted into the ring to which the reporting Ring

Monitor is attached. Once the Recovery ASIC is inserted into that ring, the DRA will be placed downstream of the last port of the module on the beaconing ring. Also, the URA will be inserted into the backup path if ports 17 and 18 are configured as trunk ports.

Similar to the beacon recovery on the module switching module, the DRA will start transmitting Beacon type 1 MAC frames when it sees a Beacon MAC frame. But the difference is that the Recovery ASIC will use the ring monitors to establish the fault domain.

There is a ring monitor associated with each port and each of them is polled by the Recovery ASIC to find the last one to see the beacon type 1 MAC frame that was sent by DRA. The fault domain is the port downstream from the ring monitor.

Once the fault domain is established, the faulty port will be wrapped.

8.10 Address-to-Port Mapping for Module Switching Modules

To discuss the address-to-port mapping on the module switching module, we will use Figure 97 on page 159 as an example.

Note that the same Recovery ASIC that is used for beacon recovery is used to provide the address-to-port mapping facility on the 8260.

As mentioned in 8.1.2.1, “Active Monitor” on page 130, every seven seconds the active monitor starts a neighbor notification process. All the stations attached to the ring will take part in the neighbor notification, enabling each station to learn its NAUN.

Note

Although the URA and DRA have a MAC address, they do not participate in the neighbor notification process. In other words, they do not issue AMP or SMP MAC frames and do not copy them either.

One of the functions of the Recovery ASIC is to monitor for AMP and SMP MAC frames and use this process to build its address-to-port map.

To build the address-to-port map, URA/DRA listen to the AMP and SMP MAC frames looking for the address-recognized and frame-copied bits on these frames. On each module, URA will be the first to see these frames enter the module and DRA will be the last to see these frames leave the module.

URA ignores all the AMP/SMP MAC frames which have the A and C bits set to B′1′, because these are the frames which have been recognized and copied by the stations which are located upstream of URA such as stations attached to other token-ring modules on this 8260. In our example, the URA in ″TR Module 2″ will ignore the AMP/SMP MAC frames issued by station ″A″, ″B″ and ″C″, as they will have A/C bits set to B′1′ by the time they have been seen by URA in ″TR Module 2″. But, as soon as the URA sees an AMP/SMP MAC frame with the A/C bits set to B′0′, it realizes that this frame has been issued by its NAUN. In this example, it would be the AMP/SMP MAC frame issued by station ″D″.

Now, DRA in ″TR Module 2″ starts tracking the stations that are involved in the neighbor notification process. The tracking will stop when the DRA in ″TR Module 2″ encounters an AMP/SMP MAC frame with the A/C bit set to B′0′, that is, AMP/SMP MAC frame issued by the NAUN to DRA. In this example, that would be the AMP/SMP MAC frame issued by station ″H″.

The stations that take part in the neighbor notification from the time that the URA sees an AMP/SMP MAC with the A/C bit set to B′0′ until the time DRA sees an AMP/SMP MAC with the A/C bit set to B′0′ (stations ″E″ thru ″H″ in our example) are the stations attached to this specific module (″TR Module 2″). These stations will then be associated with the ports that have a raised phantom voltage on the module. In this manner, the Recovery ASIC in each module is able to build the address-to-port map for its portion of the ring.

You can display the address-to-port map using the following DMM command:

```
SHOW RING_MAP TOKEN_RING LOGICAL token_ring_n or

SHOW RING_MAP TOKEN_RING LOGICAL isolated_n {slot}
```

An example of the output for this command for a module switching module with two active ports is shown in Figure 98.

```
8260> show ring_map token_ring logical token_ring_1


Token Ring Logical Map for Network TOKEN_RING_1

MAC Address           Slot      Port
-----------------     -----     ----
02-00-00-c0-cc-1c     05.01     1
08-00-8f-40-01-a6     05.01     3

8260>
```

Figure 98. Address-to-Port Map Display for a Module Switching Module

When a new station on the module inserts into the ring, it raises a phantom voltage. The Recovery ASIC waits for the next neighbor notification process to occur to determine the new MAC address and associates that MAC address with the new port.

8.10.1.1 Support for Fan-Out Devices

The 8260 token-ring modules provide support for the attachment of up to a maximum of 8 stations to a single port through the use of fan-out devices (splitters).

Note

Currently, the 8260 only supports the fan-out devices and splitters that provide a phantom signal.

To understand how the address-to-port map is built for the fan-out attached devices, let′s assume that the module shown in Figure 99 on page 162 has a fan-out device attached to its second port and currently there is only a single station (station ″B″) attached to the fan-out device. This is like having no fan-out

device on that port and therefore, the Recovery ASIC will be able to build the address-to-port map by listening to neighbor notification process as described above.

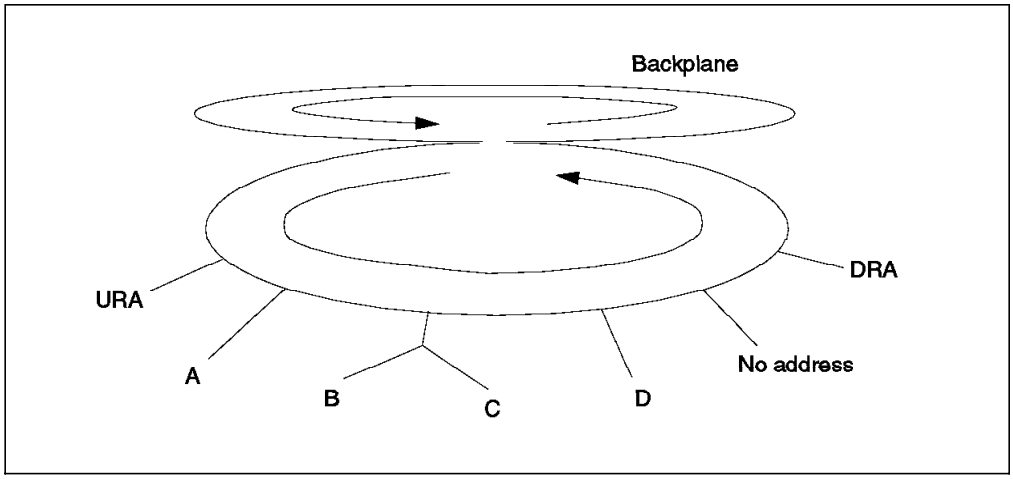


Figure 99. Address-to-port Mapping on Module Switching Modules for Fan-Out Attached Devices

Now, let′s assume that a second station (station ″C″) attaches to the fan-out device. In the next neighbor notification process the Recovery ASIC will detect that there is a new MAC address (station ″C″) in the ring but there is no new phantom voltage raised. It, therefore, assumes that the new station is attached to a port which already has a raised phantom signal (that is, the new station is attached via a fan-out device). By looking at its current address-to-port map, the Recovery ASIC can determine between which two existing MAC addresses the new MAC address has been inserted. In this example, they would be station ″B″ and station ″D″. If these two MAC addresses are on two different ports (which is the case in this example), it concludes that the new MAC address must be on the port associated with one of those two MAC addresses. The Recovery ASIC, then wraps all the ports on the module and the backplane and tests each of the two suspected ports individually by sending a Duplicate Address Test MAC frame to the new address. The received frame will be examined to see if the A/C bits are set to B′1′. If yes, then the station is on that port, and the Recovery ASIC will update its address-to-port map and then unwraps all ports.

An example of the ″ring_map″ display for a module switching module with a fan-out device attached to port 2 is shown in Figure 100 on page 163. Note that there were two stations attached to the fan-out device when this display was taken.

```
8260> show ring_map token_ring logical token_ring_1


Token Ring Logical Map for Network TOKEN_RING_1

MAC Address           Slot      Port
----------------      -----     ----
02-00-00-c0-cc-1c     05.01     1
02-00-00-c0-cc-0a     05.01     2
02-00-00-e0-9c-10     05.01     2
08-00-8f-40-01-a6     05.01     3

8260>
```

Figure 100. Address-to-Port Map Display for Fan-Out Attached Devices

There could be situations, where the two MAC addresses between which the new station is inserted are on the same port. This could happen, for example, when two stations are currently attached to a fan-out device′s ports 1 and 3 and a third station inserts between them on port 2 of the fan-out device. In this case, the Recovery ASIC concludes that the new station is on the same 8260 port as the two existing stations and will not go through the Duplicate Address Test procedure described above.

Note

With fan-out devices, the phantom signal on the port attaching the fan-out device to the hub will be raised when the first station attached to the fan-out device inserts into the ring. Therefore, a port connecting a fan-out device with no active station will be in ″no phantom″ status and will have no entry in the address-to-port map table.

Note: To allow the token-ring passive modules to perform address-to-port mapping, when splitters and fan-out devices are used, you must issue the following command:

```
SET NETWORK TOKEN_RING token_ring_n MISMATCH_RESOLUTION enable
```

8.10.1.2 Support for MAC-less Stations

The 8260 token-ring modules support the attachment of the MAC-less stations (token-ring trace tools such as IBM DataGlance) without any specific action required on the part of the user.

To support the MAC-less stations, if the Recovery ASIC detects the raising of a phantom voltage on a port and then notes that the neighbor notification process does not show any new MAC address associated with the new phantom voltage, it assumes that the attached station to this port does not have a MAC address and therefore, it sets an address of all zeros for the new port.

An example of the ″ring_map″ display for a module switching module with an IBM DataGlance attached to port 4 is shown in Figure 101 on page 164.

```
8260> show ring_map token_ring logical token_ring_1


Token Ring Logical Map for Network TOKEN_RING_1

MAC Address           Slot      Port
-----------------     -----     ----
02-00-00-c0-cc-1c     05.01     1
02-00-00-c0-cc-0a     05.01     2
02-00-00-e0-9c-10     05.01     2
08-00-8f-40-01-a6     05.01     3
00-00-00-00-00-00     05.01     4

8260>
```

Figure 101. Address-to-Port Map Display for MAC-less Stations

8.11 Address-to-Port Mapping for Per-Port Switching Modules

The per-port switching modules take advantage of the Ring Monitor function to build an address-to-port map.

The Ring Monitor function on each port is normally situated upstream of its associated port and listen for the neighbor notification process looking for AMP/SMP MAC frames, as shown in Figure 102.

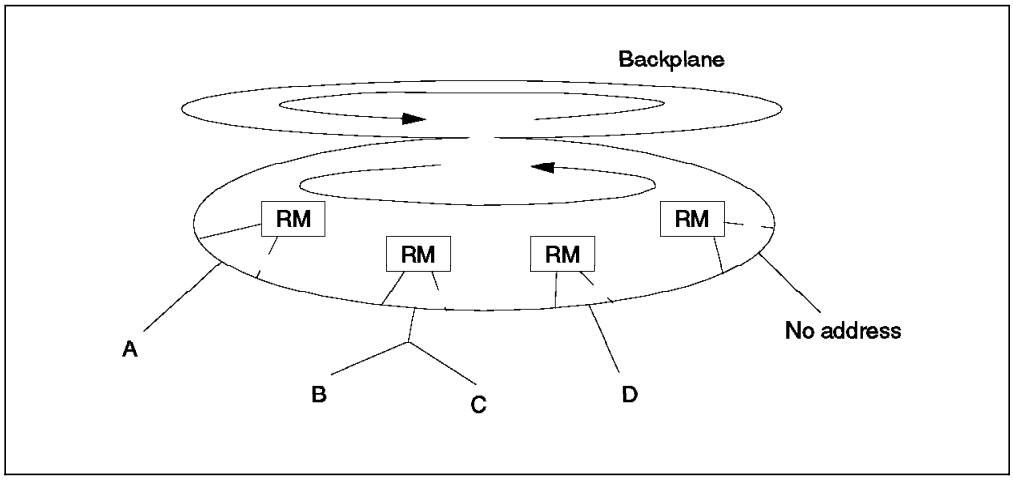


Figure 102. Address-to-Port Mapping on Per-Port Switching Modules

Ring Monitor ignores all the AMP/SMP MAC frames that have A/C bit set to B′1′, but as soon it sees an AMP/SMP with the A/C bit set to B′0′ (this frame is issued by the station immediately upstream of this Ring Monitor) it moves to the downstream side of its associated port and tracks the AMP/SMP MAC frame.

After moving downstream of its port, one of the following may happen:

1. The Ring Monitor will not see any AMP/SMP frame by the time that it is asked by the Ring Monitor downstream of it to move back upstream of its associated port. This means that there is a MAC-less station attached to that port.

   Note: The MAC-less stations do not send AMP/SMP frames.

2. An AMP/SMP MAC frame with the A/C bit set B′0′ is seen. This indicates that there is only one station attached to this port and the address of that station is one which is seen in the AMP/SMP MAC frame with the A/C bit set to B′0′. In this case, the AMP/SMP MAC frame sent by the upstream station is copied by the station attached to this port. Then the station attached to this port has issued its own AMP/SMP MAC frame which will pass this Ring Monitor with the A/C bit set to B′0′. The source address in this AMP/SMP MAC frame is the address of the station attached to this port.
3. Several AMP/SMP MAC frames with the A/C bit set to B′1′ are seen followed by an AMP/SMP MAC frame with the A/C bit set B′0′.

   This indicates that there are several stations attached to this port via a fan-out device and the addresses of these stations are the source addresses in the AMP/SMP MAC frames.

   In this case, the AMP/SMP MAC frame sent by the upstream station is copied by the station attached to the first port of the fan-out device and the AMP/SMP MAC frame issued by that station is subsequently copied by the station attached to the second port of the fan-out device and so on. The source addresses in all the AMP/SMP MAC frames with the A/C bit set to B′1′ plus the source address of the AMP/SMP MAC frame with the A/C bit set to B′0′ show addresses of the stations attached to this port (via the fan-out device) and are used by the Ring Monitor to build the address-to-port map for this port.

   Note

   A fan-out device may support more than 8 stations which will result in the Ring Monitor seeing as many AMP/SMP frames as the number of stations. However, the Ring Monitor will only save the address of the first eight stations.

The AMP/SMP issued by the last (or the only) station on each port will pass the Ring Monitor function on that port and will immediately be seen by the Ring Monitor function on the next port downstream from this port. As soon as the Ring Monitor on the downstream port sees this AMP/SMP MAC frame with the A/C bit set to B′0′, it moves downstream of its associated port and will then signal the Ring Monitor on the upstream port which currently is situated downstream of its associated port to move to the upstream of its associated port to prepare for the next round of neighbor notification as well as assisting the Recovery ASIC with the beacon recovery process.

The above procedure will be repeated on all the ports helping the Recovery ASIC to build an accurate address-to-port map for all the ports on the module.

An example of the output for this command is shown in Figure 103 on page 166.

```
8260> show ring_map token_ring logical token_ring_2


Token Ring Logical Map for Network TOKEN_RING_2

MAC Address           Slot      Port
-----------------     -----     ----
02-00-00-e0-9c-10     06.01     1
02-00-00-c0-cc-68     06.01     7
00-00-00-00-00-00     06.01     10
08-00-8f-d0-90-fa     06.02     N/A
02-00-00-66-88-8d     06.01     15

8260>
```

Figure 103. Address-to-Port Map Display for a Per-Port Switching Module

Note that in the above display, the module 6.01 is an active per-port switching module and the module 6.02 is a T-MAC installed on this active per-port switching module.

8.11.1.1 Support for Fan-Out Devices

As mentioned in the above procedure, the active per-port switching modules support the attachment of up to a maximum of 8 stations to a single port through the use of fan-out devices.

8.11.1.2 Support for MAC-Less Stations

The active per-port switching supports the attachment of MAC-less stations to all ports except the last port. This is because the Ring Monitor on the last station of a per-port switching module (that has a MAC-less station) will move downstream of its associated port when it sees an AMP/SMP MAC frame with the A/C bit set to B′0′ and begins trapping the AMP/SMP MAC frames that it sees. Since the station attached to this port does not have a MAC address (does not participate in the neighbor notification) and does not copy any AMP/SMP MAC frame, the Ring Monitor will not see any AMP/SMP MAC frame with the A/C bit set to B′1′ and will remain on the downstream side of this port and as there is no Ring Monitor downstream from this one on the module to ask it to move back upstream of this port, the map for the last port will not be accurate.

Note

The active token-ring modules provide RI/RO ports which allow you to connect your 8260 to other hubs. Note that in this case, no address-to-port mapping is done for the RI/RO ports. The address-to-port map which will be built and maintained by each module are only for the stations which are attached to the module via lobe ports.

8.12 IEEE 802.5C Recommended Practice for Dual Ring Wrapback Reconfiguration

Dual-ring recovery as recommended by IEEE 802.C is intended for applications that require very high availability and recovery from media and station failures.

As illustrated in Figure 104 on page 167, the dual-ring topology consists of two counter-rotating rings that provide interconnection for both dual-ring and single-ring stations. One of the rings is designated as the *primary ring* and the other ring is designated as the *secondary ring*.

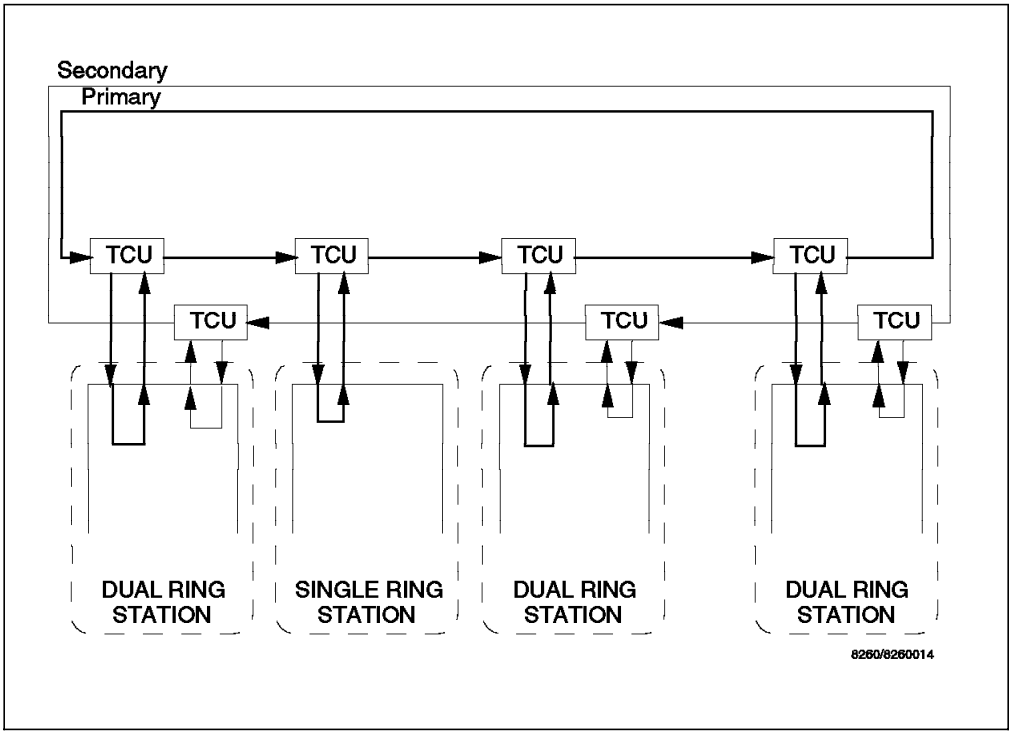


Figure 104. Dual-Ring Topology

Normally, the primary ring is the operational ring and no data other than the MAC frames flow on the secondary ring.

Single-ring stations can only be connected to the primary ring through a Trunk Coupling Unit (TCU) and operate exactly as specified in the IEEE 802.5 standard. Dual-ring stations on the other hand are connected to both the primary ring and secondary ring through two TCUs.

Dual-ring reconfiguration employs *wrapback* to provide for recovery from all forms of signal loss failures and from trunk line failures not covered by the IEEE 802.5 standard.

The wrapback method restores normal operation by interconnecting the two rings on each side of the failure as shown in Figure 105 on page 168. This results in a single ring being formed from the remaining good parts of the original two rings.

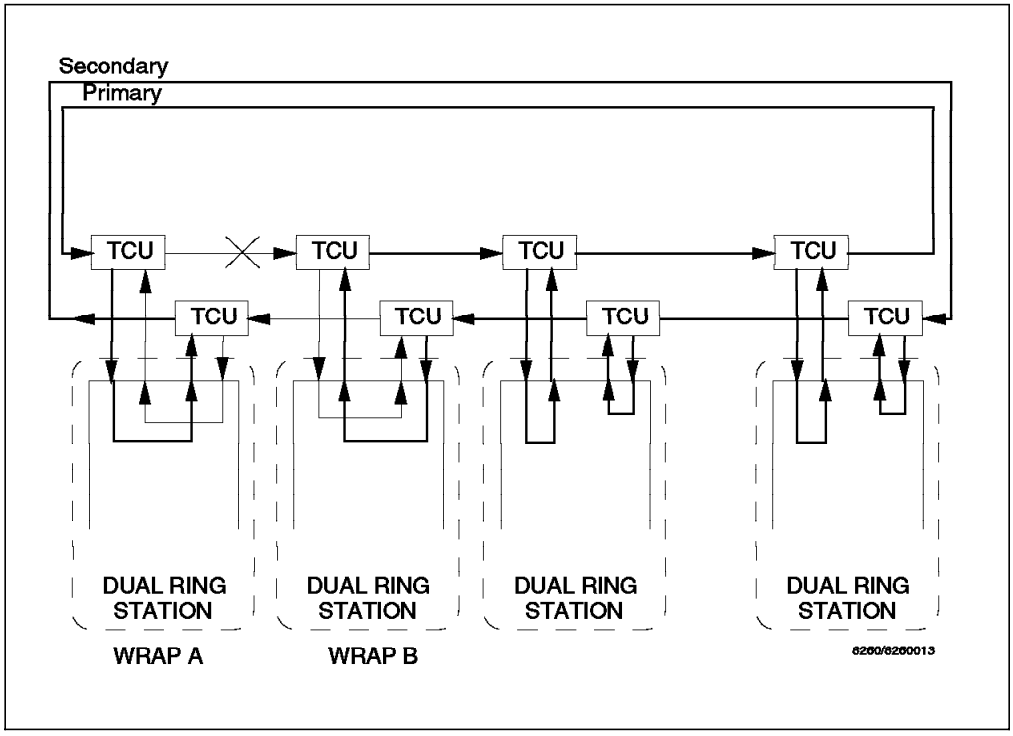


Figure 105. Wrapback in Dual-Ring Topology

8.12.1 Trunk Wrapping on the Active Per-Port Switching Modules

The 18-port active per-port switching module and the 10-port dual fiber repeater module conform to the 802.5C dual-ring reconfiguration practice.

When, during the beacon recovery process, it is determined that the fault domain is between RI and RO, the following process takes place:

1. DRA is inserted on the primary path and URA is inserted on the backup path between RI and RO ports.
2. Faulty trunk is located and wrapped using dual-ring recovery methods.
3. URA and DRA are de-inserted.
4. DMM and Merge Manager (see 8.12.3, “Merge Manager” on page 170) are notified of the action taken.

This is shown in Figure 106 on page 169.

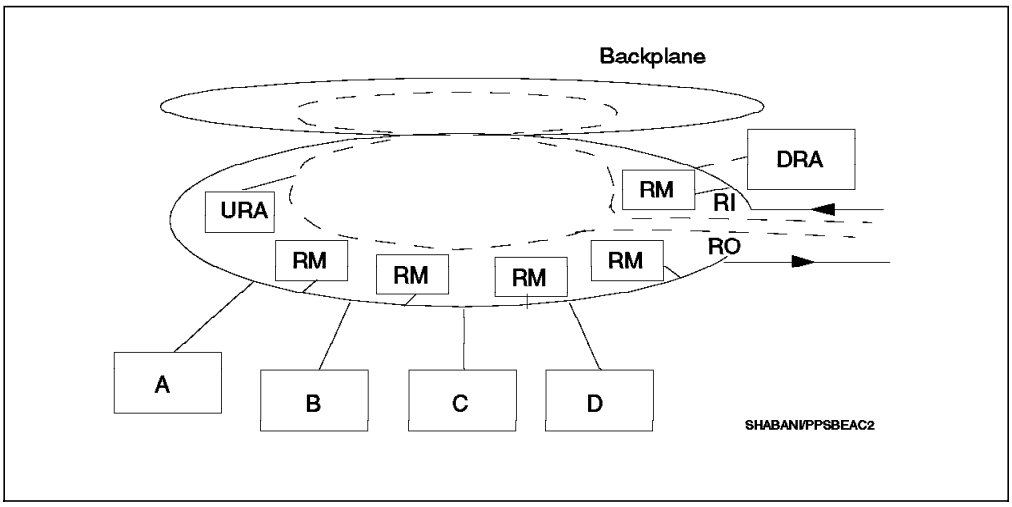


Figure 106. Trunk Wrapping in Active Per-Port Switching Module

8.12.2 Trunk Wrapping on the Active Module-Switching Modules

When, during the beacon recovery process, it is determined that the fault domain is between RI and RO, the following process takes place:

1. DRA and URA are inserted on the primary path.
2. RI/RO trunk is treated like a single lobe port. If wrapping the trunk pair fixes the fault, trunks are left wrapped.
3. URA and DRA are de-inserted.
4. DMM and Merge Manager (see 8.12.3, “Merge Manager” on page 170) are notified of the action taken.

This is shown in Figure 107.

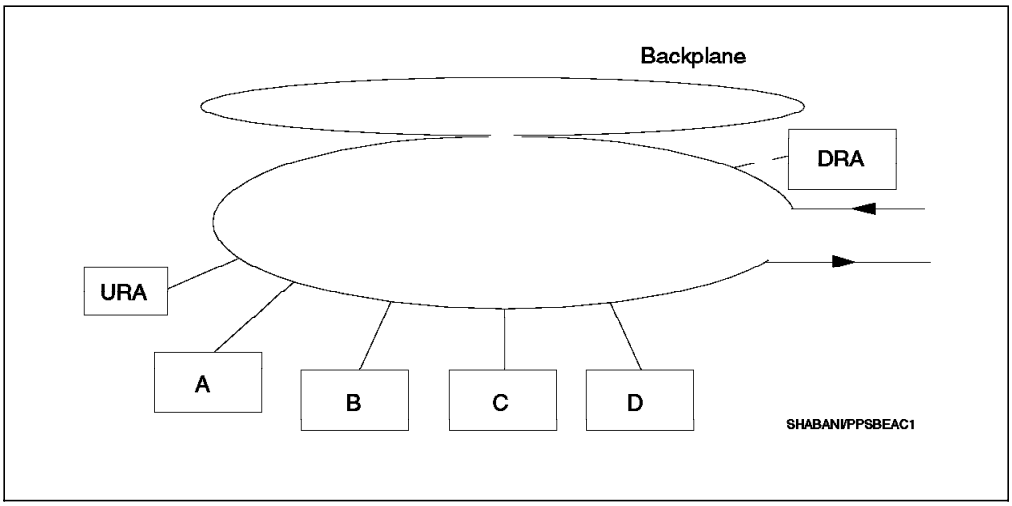


Figure 107. Trunk Wrapping in Active Per-Port Switching Module

Note

On the 18-port active module switching module, the URA cannot be switched to the backup path. This means that the operation of this module is not IEEE 802.5C conformant.

8.12.3 Merge Manager

The function of the Merge Manager is to periodically check RI and RO trunks to see if the cause of the beacon has been resolved and the trunks can be unwrapped.

Note

The Merge Manager algorithm is the same on the per-port switching modules and module-switching modules; the only difference is in the timers which determine how often the trunk test gets executed.

To check the trunks, the Merge Manager creates a ring segment with the trunk under the test and the URA.

The URA checks to see whether this ring segment either has an Active Monitor (indicating a healthy ring) or is capable of passing traffic generated by the URA. If the segment passes one of these tests, the trunk is deemed to be recovered and is unwrapped. If it fails the test, retry will be attempted at intervals described below.

8.12.4 Trunk Unwrapping on the Per-Port Switching Modules

For trunks attached to the 18-port active per-port switching module and the 10-port dual fiber repeater module, merging (unwrapping) is attempted:

- After 5 seconds
- After 30 seconds
- Every 5 minutes

Because these modules have switching capability, the Recovery ASIC may be switched onto the faulty segment without disturbing the rest of the stations on the module. Thus, we can test faulty segments without disrupting the working ring segments.

8.12.5 Trunk Unwrapping on the Module-Switching Modules

For trunks attached to the module-switching modules merging (unwrapping) is attempted:

1. Every 5 seconds
2. Every 30 seconds
3. After 5 minutes
4. After 20 minutes
5. Never again. This means that manual intervention (using DMM commands) will be necessary to unwrap RI and/or RO ports.

Because these modules do not have switching capabilities, the URA cannot be switched onto the faulty segment. In order to execute the unwrapping tests, the module must wrap the backplane and wrap all the lobe ports. This allows the URA to be on a segment isolated with the trunk under the test. Obviously, this is disruptive to the stations on the module, so it is not desirable to try this every 5 minutes.

Note

URA cannot transmit Downstream Converter Presence because the Recovery ASIC MAC cannot transmit on token. Also, if LNM is on the ring, it does not get a MAIN RING PATH WRAPPED TO BACKUP alert.

Chapter 9. 8260 Token-Ring Modules

This chapter will describe the token-ring modules for the 8260 multiprotocol intelligent switching hub. Each module will be described along with its features and the necessary steps required to configure these modules. Currently, the available 8260 token-ring modules are:

- 18-port Active Per Port Switching Module
- 18-port Active Module Switching Module
- Dual Fiber Repeater Module
- 20-port Passive Module Switching Module
- Jitter Attenuator Daughter Card

9.1 Introduction

The 8260 token-ring modules can only be connected to the token-ring segments on the ShuntBus. They cannot be attached to the token-ring segments on the Enhanced TriChannel. You can also install and use any 8250 token-ring module in the 8260 multiprotocol intelligent switching hub. The 8250 token-ring modules can only be connected to the token-ring segments on the Enhanced TriChannel. Therefore, a token-ring segment on the 8260 can consist of 8250 or 8260 token-ring modules. However, you may use RI/RO connections, bridges or routers to connect the 8260 token-ring segments consisting of 8260 modules to the token-ring segments consisting of 8250 modules.

For information about 8250 Ethernet modules please refer to *IBM 8250 Intelligent Hub and IBM HUB Management Program/6000,*GG24-4033.

9.2 Configuring Token-Ring Network Parameters

Before discussing the individual 8260 token-ring modules and how to configure them, this section describes the parameters that may be configured for each network segment to which the 8260 token-ring modules and ports are to be attached.

The following is the summary of parameters that may be configured for each token-ring segment:

- Enable/disable automatic beacon recovery

  Use the following command to enable/disable the automatic beacon recovery for each segment to which the ports or modules are to be attached:

  ```
  SET NETWORK {network} BCN_RECOVERY {enable|disable}
  ```

  Note that if you disable this feature, any beacon condition on the network will disrupt the operation of the network until you remove the source of beaconing from the ring.

- Set the ring speed

  You must set the ring speed for the backplane or isolated segment using the following command:

  ```
  SET NETWORK {network} RING_SPEED {4_mbps|16_Mbps}
  ```

Once the ring speed for the network is set, each port, trunk or module assigned to that network will assume the speed of the network.

- Enable support for splitters and fan-out devices

  If you are planning to attach passive modules to a segment and there are splitters and fan-out devices attached to the ports of the passive module, you must issue the following command to ensure that an accurate port-to-address mapping is performed on the network:

  ```
  SET NETWORK {network} MISMATCH_RESOLUTION {enable}
  ```

  Note: This command is not required if the network consists of active modules only.

9.3 8260 18-Port Active Per-Port Switching Module

This module is a single-slot module that supports 18 active ports. The main features of this module are:

- 18 ports with shielded RJ-45 connectors.
- Each port has its own DPLL, which actively re-times and re-generates the signal on that port. This provides longer lobe distances on both UTP and STP. For the lobe distances supported on the active ports, please refer to Table 26 on page 143.
- Each port can be connected to one of the 10 token-ring segments on the ShuntBus or one of the 11 isolated segments on the module. All the ports can be connected to a maximum of 11 segments consisting of backplane and isolated segments.

  Note: When you use a backplane (or isolated) segment the equivalent isolated (or backplane) segment is not available. For example if one or more ports are assigned to token_ring_1 segment, no port can be assigned to isolated_1 segment.
- Simultaneous UTP and STP cabling is supported on the module. Also, UTP and STP attached stations can be connected to the same segment.
- Ports 17 and 18 can optionally be configured to be used as RI/RO ports for connection to another hub. This module supports RI/RO connections to an 8228, 8230, 8250 and 8260.
- Support for beacon recovery using the Recovery ASIC which is implemented on the module. Unlike 8250, there is no need for a management module to resolve beacon conditions.
- Support for address-to-port mapping using the recovery ASIC.
- Support for fan-out devices and splitters for attaching up to 8 stations to each port. Note that the fan-out device or the splitter is required to provide a phantom signal; therefore, 8228 cannot be used as the fan-out device with this module.
- Support for connection of MAC-less stations (such as token-ring tracing tools) to all ports except port 18.
- Automatic speed detection of the attached stations so that only the stations with the correct ring speed settings can attach to the network.
- Support for simultaneous 4 and 16 Mbps token-ring networks on the module.

- When ports 17 and 18 are configured as RI/RO ports, they are fully compliant with the IEEE 802.5C (dual-ring recovery) standard.
- Support for installation of one T-MAC.
- Support for installation of one Jitter Attenuator daughter card.

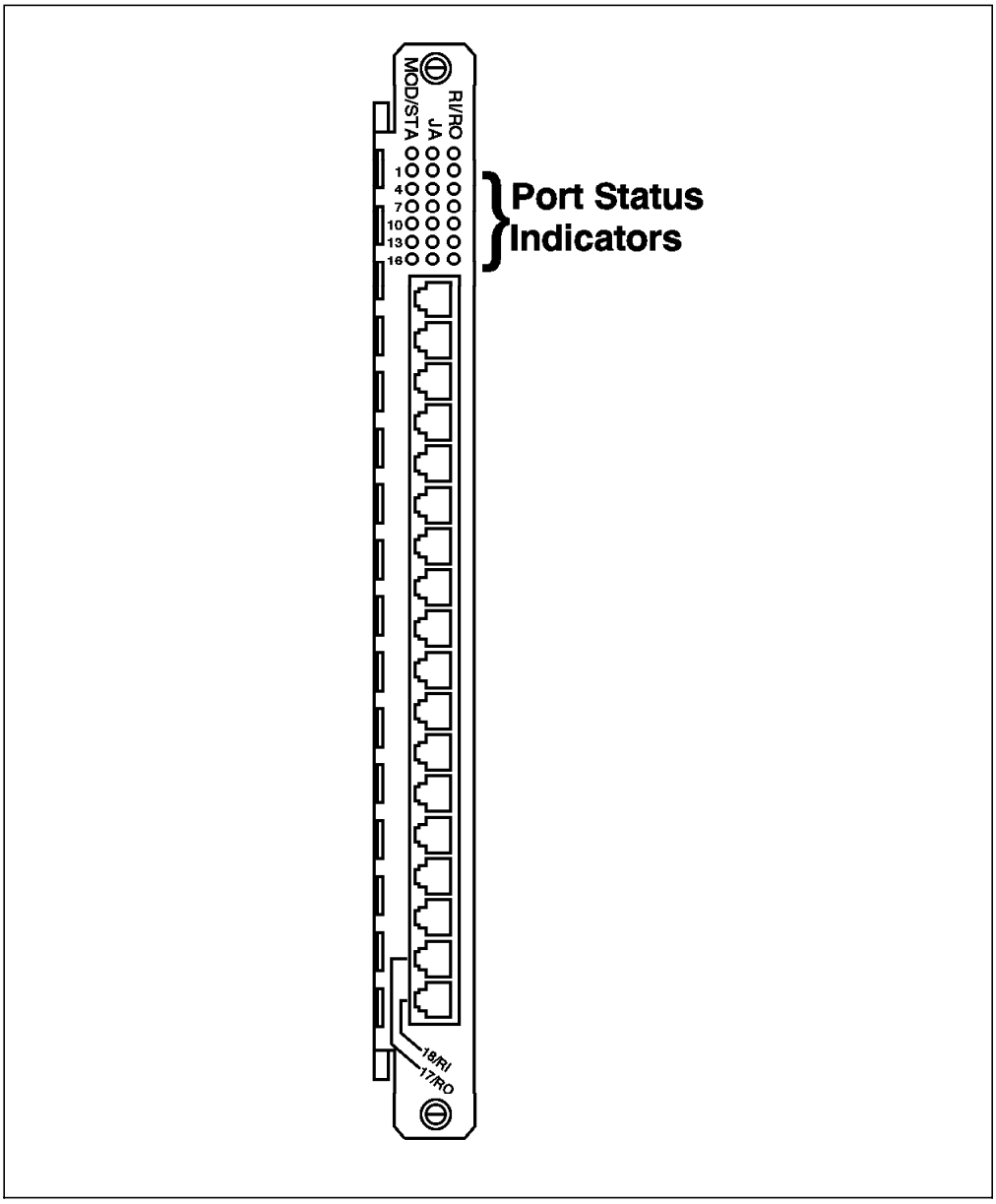


Figure 108. Front View of 18-Port Active Per-Port Switching Module

Figure 108 shows the front view of the 18-port active per-port switching module. As can be seen, this module provides LED Indicators on the front panel that allow you to monitor the status of the module and the individual ports. Table 28 on page 176 describes the meaning of these LEDs:

Table 28. 18-Port Active Per-Port Switching Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
Module Status	Green	On	Module powered up OK
		Off	No Power
		Blinking	Module failed self diagnostics
RI/RO	Green	On	Trunk enabled and operating
		Off	Trunk disabled
		Blinking	Trunk enabled but not operating normally
JA	Green	On	JADC card installed and operating normally
		Off	JADC card not installed
		Blinking	JADC card failed diagnostics
Port Status	Green	On	Port enabled and operating normally on the ring
		Off	Port disabled
		1 blink	Port enabled, no phantom
RI/RO	Green	On	Ports 17 and 18 are RI/RO ports
		Off	Ports 17 and 18 are lobe ports

Figure 109 shows the side view of the 18-port active per-port switching module. As can be seen, in addition to the 11 isolated segments and the mounting for one T-MAC, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored unless ″DIP_CONFIGURATION″ is enabled for DMM. For more information, please refer to 4.2.4.4, “ Configuring DMM Device” on page 50.

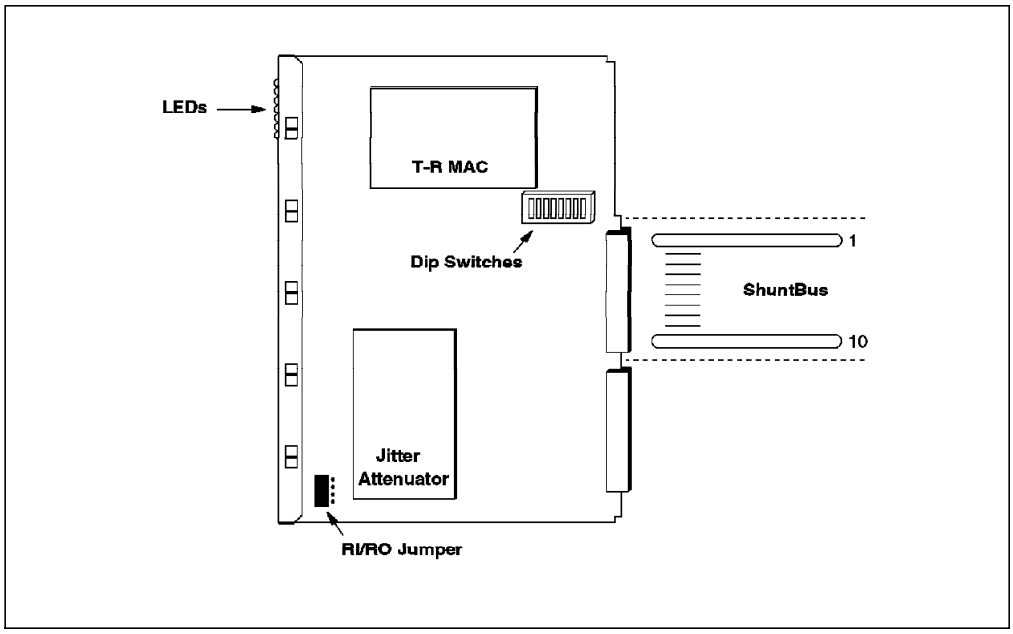


Figure 109. 18-Port Active Per-Port Switching Module Side View

The DIP switches let you perform the following:

- Use DIP switch positions 1 through 4 to assign all the ports on the module to one of the backplane segments or isolated-1 segment. Note that when using DIP switches, all the ports will be assigned to the same segment, so you cannot do per-port switching when using DIP switches for configuring your 8260 modules.

  Table 29 shows the meaning of settings for DIP switches 1 thru 4:

Table 29. 18-Port Active Per-Port Switching Module

Network Selection	Switch 1	Switch 2	Switch 3	Switch 4
token_ring_1	ON	OFF	OFF	OFF
token_ring_2	OFF	ON	OFF	OFF
token_ring_3	ON	ON	OFF	OFF
token_ring_4	OFF	OFF	ON	OFF
token_ring_5	ON	OFF	ON	OFF
token_ring_6	OFF	ON	ON	OFF
token_ring_7	ON	ON	ON	OFF
token_ring_8	OFF	OFF	OFF	ON
token_ring_9	ON	OFF	OFF	ON
isolated_1	OFF	OFF	OFF	OFF

  By default, the module is shipped from the factory with the DIP switches set for token_ring_1.

- Use DIP switch position 5 to choose if the module is going to use the Non-Volatile RAM (ON position) or DIP switch settings (OFF position) for its configuration. Note that if there is a management module installed in the 8260, this DIP switch determines which configuration (NVRAM or DIP switch setting) will be sent to the management module. The actions taken by the management module, upon receipt of this information are described in 4.2.4.4, " Configuring DMM Device" on page 50. By default, DIP switch 5 is set to NVRAM.
- Use DIP switch position 8 to set the ring speed to 4 Mbps (ON) or 16 Mbps (OFF). The module is shipped from the factory with the speed set to 16 Mbps.

9.3.1 Configuring the 18-Port Active Per-Port Switching Module

To configure this module you must do the following:

1. Before installing the module in the 8260, use the onboard jumpers on the module to determine whether ports 17 and 18 are used as lobe ports or RI/RO trunk ports. The onboard jumpers are shown in Figure 110 on page 178.

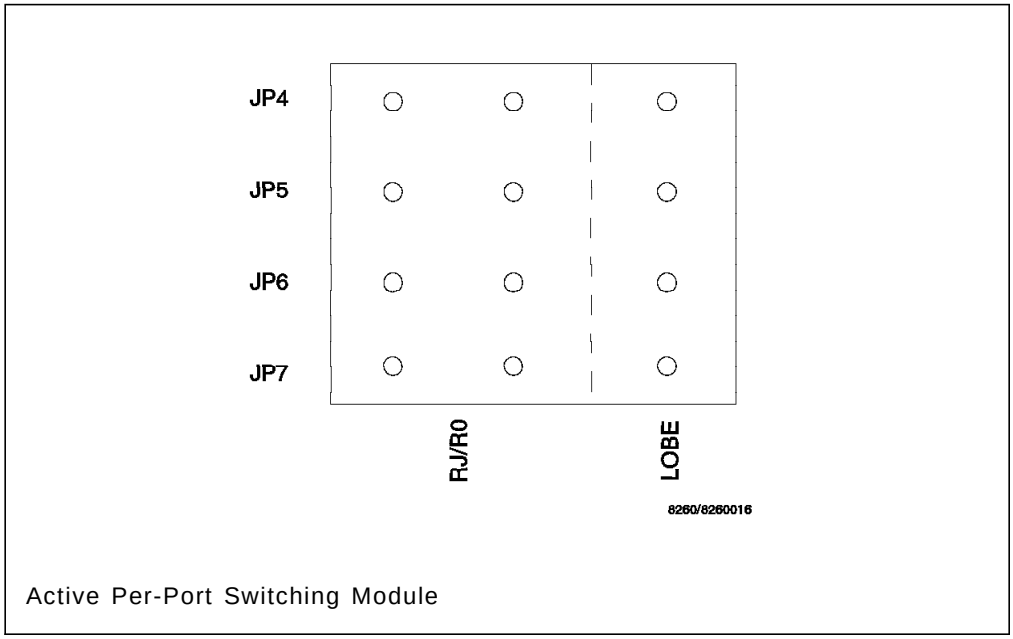


Figure 110. Onboard Lobe/Trunk Jumpers on 18-Port

Note that setting the jumpers to the left selects RI/RO and setting the jumpers to the right selects lobe ports.

2. Set beacon threshold for the module.

   When a beaconing condition is detected on a port, the port is wrapped by the recovery ASIC. The port is unwrapped when a transition of phantom is detected or when the port is disabled and then re-enabled by the administrator.

   The number of times that a phantom transition is allowed to cause a port to unwrap is determined by the bcn_threshols parameter which can be set for each module using the following command:

   ```
   SET MODULE {slot.port} BCN_THRESHOLD {0-255}
   ```

   Once the threshold is exceeded, the port or trunk remains wrapped until the user disables and re-enables the port. While wrapped, the port status is *BCN THRES EXCEEDED*.

   Note: The bcn_threshold is reset whenever a port on the module successfully inserts into the ring, or the module is reset.

3. Enable/disable static switch for each port.

   If you want the user of a port to power down the station (drop the phantom signal) before that port can be switched to another network segment, you must enable the *static_switch* for the specified port using the following command:

   ```
   SET PORT {slot.port} STATIC_SWITCH {enable|disabled}
   ```

   Once the static_switch is disabled, the port can be switched to another segment without dropping the phantom signal. For more information about static_switch please refer to 8.6.2, “Static Switch on the Per-Port Switching Modules” on page 145.

4. Assign ports to network segments.

Use the following command to assign each port on the module to one of the backplane segments on the ShuntBus or isolated segments on the module:

```
SET PORT {slot.port} NETWORK {network}
```

5. Assign RI/RO ports to network segments.

   If you have configured ports 17 and 18 as RI/RO trunks, you can assign them to a network using the following command:

   ```
   SET TRUNK {slot} RING_IN NETWORK {network} or
   SET TRUNK {slot} RING_OUT NETWORK {network}
   ```

   In this command you do not need to specify port number for the trunk as port 17 is always RING_OUT and port 18 is RING_IN.

   Note: If you assign a RING_IN (or RING_OUT) trunk to a segment, the other trunk will automatically be assigned to the same segment.

6. Set compatibility mode for the trunk ports.

   Ports 17 and 18, when configured as trunks, can be used to connect your 8260 to another hub. Depending on the hub to which the trunk is attached you must set the following compatibility mode for the trunk:

   - 8260

     This is used when the trunk is connected to another 8260.

   - ONcore

     This is used when the trunk is connected to a Chipcom ONcore switching hub.

   - 8250

     This is used when the trunk is connected to an 8250 or 8228.

   - ONline

     This is used when the trunk is connected to a Chipcom ONline switching hub.

   - 8230

     This is used when the trunk is connected to an 8230.

   All of the current 8260 trunk compatibility modes can be summarized as two different modes:

   a. 8250/8230/ONline

      In this mode, the trunks open when enabled as long as a signal can be passed through the trunk connection. A jitter attenuator is also required for the trunks to unwrap. There is no phantom involved, and there is no special protocol involved. Wrapping of the port in the case of a fault is triggered only by the presence of beacon frames. If the module detects a beaconing ring and decides the problem is being caused by someone or something attached to it, it will first wrap the trunks and see if the ring recovers. If it does, the module goes to a ″schedule″ for retesting the trunks to see when it recovers. If the module does not recover, it goes on to removing other ports on that ring until the ring recovers.

   b. 8260/ONcore

      In this mode, phantom is generated on the RI trunk and/or required to be detected on the RO port for the RI trunk and/or required to be detected on the RO port for the trunks to insert. Also a jitter attenuator is not

required. If a trunk fault appears which disrupts phantom drive, the trunk will wrap immediately. The module never goes to beacon recovery because the problem is corrected before that happens. If, for any reason, phantom is not disturbed by the fault, beacon recovery is initiated as in No. 1 above.

To set the compatibility mode for a trunk, you can use the following command:

```
SET TRUNK {slot} RING_IN COMPATIBILITY_MODE {mode} or
SET TRUNK {slot} RING_OUT COMPATIBILITY_MODE {mode}
```

7. Enable/disable trunks

   If ports 17 and 18 are configured as RI/RO trunks, they can be enabled/disabled using the following command:

   ```
   SET TRUNK {slot} RING_IN MODE {enable|disable} or
   SET TRUNK {slot} RING_OUT MODE {enable|disable}
   ```

8. Enable/disable ports

   Each port can be enabled/disabled using the following command:

   ```
   SET PORT {slot.port} mode {enable|disable}
   ```

9.4 8260 18-Port Active Module Switching Module

This module is identical to the 18-port active per-port switching module with the exception that it does not support the per-port switching feature. This means that all the ports on this module can only be assigned to the same segment on the backplane or can all be isolated.

9.4.1 Configuring the 18-Port Active Module Switching Module

Configuration of this module is identical to the configuration of the 18-port active per-port switching module with the exception that you must assign the module to a backplane segment or an isolated network using the following command:

```
SET MODULE {slot.subslot} NETWORK {network}
```

9.5 8260 20-Port Passive Module Switching Module

This is a single slot module that supports 20 passive ports. This is a module switching module, which means that all the ports must be attached to the same segment. The main features of this module are:

- 20 ports with shielded RJ-45 connectors.
- A single DPLL which is implemented on the module will remove the jitter before passing the signal to the 8260 backplane. Note that unlike the active modules, the individual ports do not have their own DPLL.
- The module can be assigned to any of the 10 token-ring segments on the ShuntBus or can be isolated. When isolated, all the stations attached to this module can communicate with each other but not with the stations attached to the other modules.
- Support for both UTP and STP cabling. However, you cannot mix both cabling types on the same module simultaneously.
- Support for beacon recovery using the Recovery ASIC which is implemented on the module. For more information about beacon recovery support on the

passive module refer to 8.9.4, “Beacon Recovery on the Module Switching Modules” on page 158.

- Support for address-to-port mapping using the Recovery ASIC.
- Support for fan-out devices and splitters for attaching up to 8 stations to each port. Note that fan-out device or splitter is required to provide a phantom signal; therefore, an 8228 cannot be used as the fan-out device with this module.
- Support for connection of MAC-less stations (such as token-ring tracing tools).
- Software-based speed detection so that only the stations with the correct ring speed settings can attach to the network. Note that the speed detection implemented on the passive module may be enabled or disabled by the user.
- Support for 4 or 16 Mbps token-ring networks.
- Support for installation of one T-MAC.
- Built-in Jitter Attenuator daughter card.

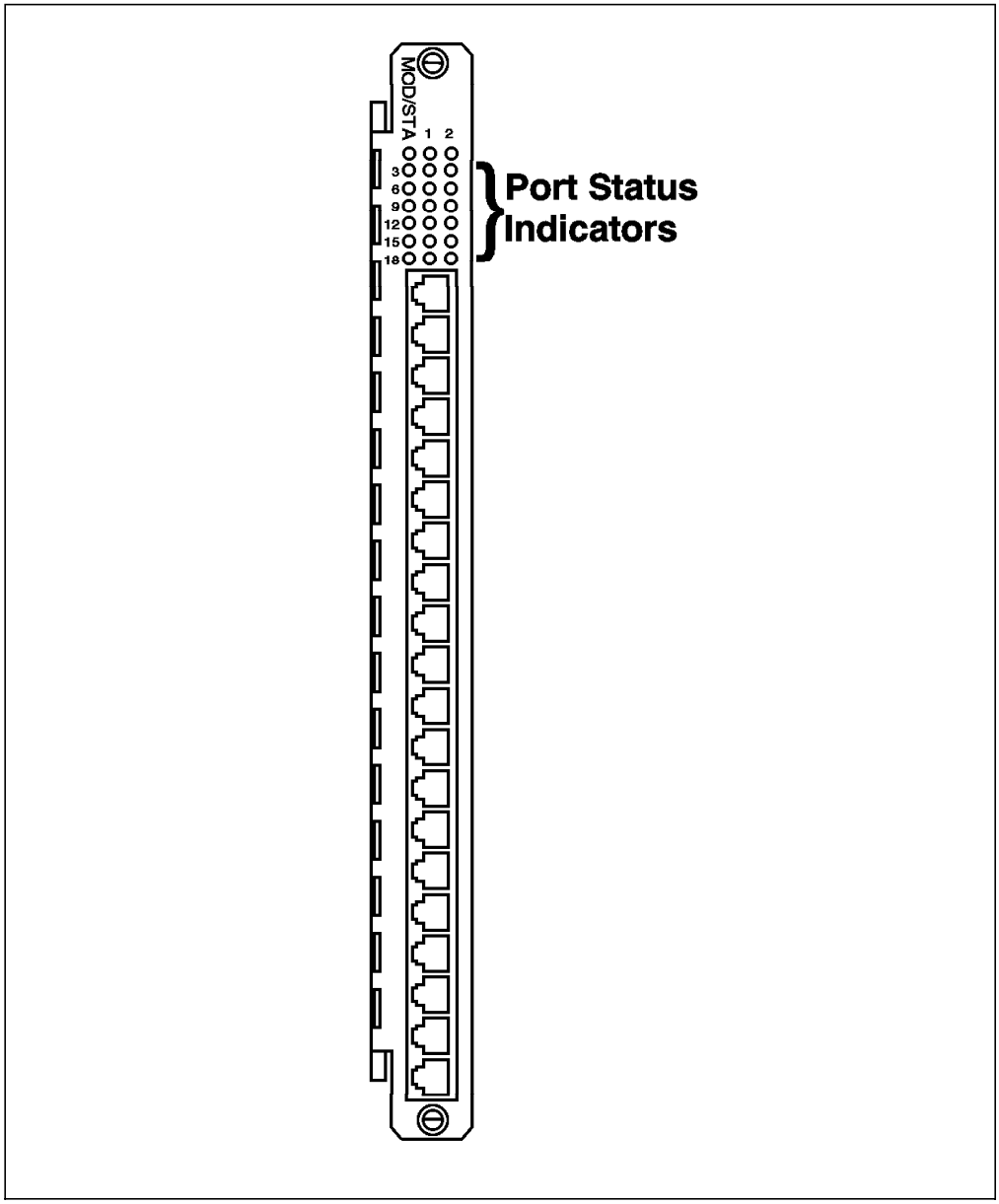


Figure 111. Front View of 20-Port Passive Module

Figure 111 shows the front view of the 20-port passive module. As can be seen, this module provides LED indicators on the front panel that allow you to monitor the status of the module and the individual ports. Table 30 describes the meaning of these LEDs:

Table 30 (Page 1 of 2). 20-Port Passive Module LED Descriptions

LED Name	Color	State	Description
Module Status	Green	On	Module powered up OK
		Off	No Power
		Blinking	Module failed self diagnostics

Table 30 (Page 2 of 2). 20-Port Passive Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
Port Status	Green	On	Port enabled and operating normally on the ring
		Off	Port disabled
		1 blink	Port enabled, no phantom

Figure 112 shows the side view of the 20-port passive module. As can be seen, in addition to the 11 isolated segments and the mounting for one T-MAC, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored unless ″DIP_CONFIGURATION″ is enabled for DMM. For more information, please refer to 4.2.4.4, " Configuring DMM Device" on page 50.

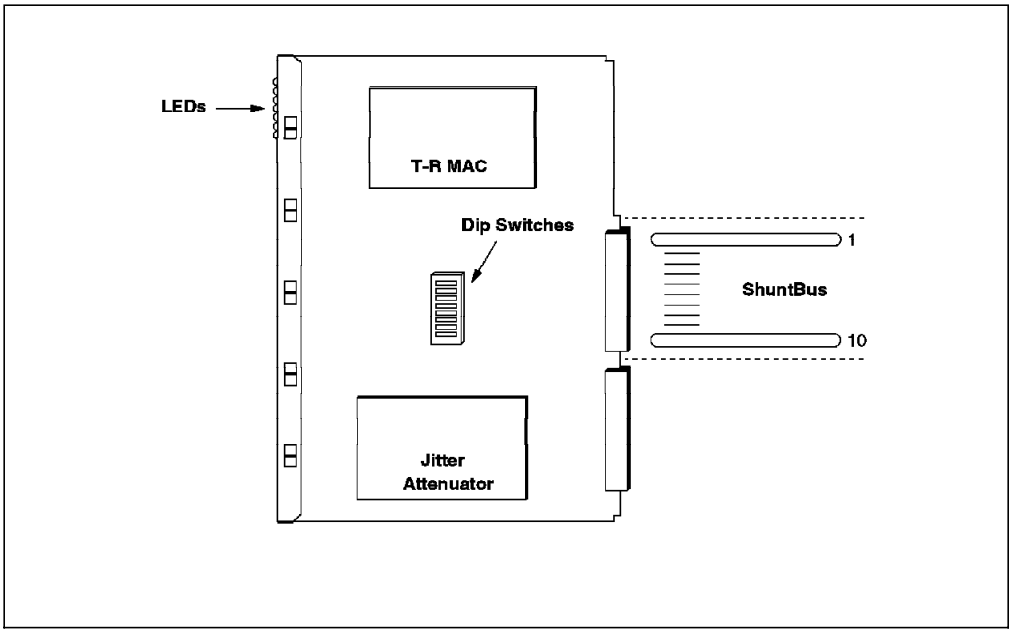


Figure 112. 20-Port Passive Module Module Side View

The DIP switch settings for this module are identical to the 18-port active per-port switching module (described in 9.3.1, "Configuring the 18-Port Active Per-Port Switching Module" on page 177) with the following exception:

- Use DIP switch position 6 to enable (OFF) or disable (ON) the speed detection on the passive module. For more information about the speed detection algorithm used by the 20-port passive module please refer to 8.8.2, "Speed Detection on Passive Modules" on page 149.

9.5.1 Configuring the 20-Port Passive Module

To configure this module you must do the following:

1. Set beacon threshold for the module.

   When a beaconing condition is detected on a port, the port is wrapped by the Recovery ASIC. The port is unwrapped when a transition of phantom is detected or when the port is disabled and then re-enabled by the user.

The number of times that a phantom transition is allowed to cause a port to unwrap is determined by the bcn_threshold parameter which can be set for each module using the following command:

```
SET MODULE {slot.port} BCN_THRESHOLD {0-255}
```

Once the threshold is exceeded, the port or trunk remains wrapped until the user disables and re-enables the port. While wrapped, the port status is *BCN THRES EXCEEDED*.

Note: The bcn_threshold is reset whenever a port successfully inserts into the ring, or the module is reset.

2. Enable/disable speed detection for each port.

   You can enable/disable speed detection for the individual ports on the passive module using the following command:

   ```
   SET PORT {slot.port} SPEED_DETECT {enable|disable}
   ```

   When enabled, speed detection prevents the stations from inserting into the ring at the wrong speed. When the incorrect speed is detected, the port is wrapped and the status of the port is changed to *SPEED MISMATCH*. The port will unwrap when a phantom transition is detected on the port or the port is disabled and then re-enabled by the administrator. For more information about speed detection, please refer to 8.8.2, “Speed Detection on Passive Modules” on page 149.

3. Set speed threshold for the module.

   You can set the number of times that a phantom transition allows a wrapped port, due to the beacon conditions, to unwrap. To do so, you can use the following command:

   ```
   SET MODULE {slot.port} SPEED_THRESHOLD {0-255}
   ```

   When this threshold is reached, the port remains wrapped with the status of *SPD THRESHOLD EXCEEDED* until the administrator disables and re-enables the port.

   Note: This threshold is reset whenever a port on the module successfully inserts into the ring.

4. Assign the module to a network segment.

   Use the following command to assign the module to one of the backplane segments or isolate it from the backplane.

   ```
   SET PORT {slot.port} NETWORK {network}
   ```

   Note: As a result of this command, all the ports on the module will be assigned to the same segment.

5. Enable/disable ports.

   Each port can be enabled/disabled using the following command:

   ```
   SET PORT {slot.port} mode {enable|disable}
   ```

9.6 8260 Dual Fiber Repeater Module

This is a single slot module that supports 10 active lobe ports and two sets of fully repeated fiber RI/RO trunk ports. This is a per-port switching module, which means that any of the lobe ports or and trunk port sets can be assigned to any of the backplane segments. The main features of this module are:

- 10 lobe ports with shielded RJ-45 connectors.
- Each lobe port has its own DPLL, which actively re-times and re-generates the signal on that port. This provides longer lobe distances on both UTP and STP. For information of the maximum lobe distances, please refer to Table 26 on page 143.
- Each lobe port can be connected to one of the 10 token-ring segments on the ShuntBus or one of the 11 isolated segments on the module.
- 2 sets of fully repeated fiber RI/RO trunk ports with ST connectors.
- Each trunk port is fully repeated and supports multimode fiber connections for 62.5/125 fiber at distances up to 2 km.
- Each set of trunk ports can be assigned to one of the 10 token-ring segments on the ShuntBus or one of the 11 isolated segments on the module.

  Note: The lobe and trunk ports can be assigned to a maximum of 11 backplane or isolated segments. When you use a backplane (or isolated) segment the equivalent isolated (or backplane) segment is not available. For example if one or more ports are assigned to token_ring_1 segment, no port can be assigned to isolated_1 segment.
- Simultaneous UTP and STP cabling is supported on the lobe ports attached to the same or different segments.
- Support for beacon recovery on both lobe and trunk ports using the Recovery ASIC which is implemented on the module.
- Support for address-to-port mapping using the recovery ASIC.
- Support for fan-out devices and splitters for attaching up to 8 stations to each port. Note that the fan-out device or the splitter is required to provide a phantom signal; therefore, the 8228 cannot be used as a fan-out device with this module.
- Support for connection of MAC-less stations (such as token-ring tracing tools) to all the lobe ports.
- Automatic speed detection of the attached stations to the lobe ports, so that only the stations with the correct ring speed settings can attach to the network.
- Simultaneous support of 4 and 16 Mbps token-ring networks on the lobe and trunk ports.
- Compliant with the 802.5C (dual-ring recovery) on the trunk ports.
- Support for installation of one T-MAC.
- Support for installation of two Jitter Attenuator daughter cards.

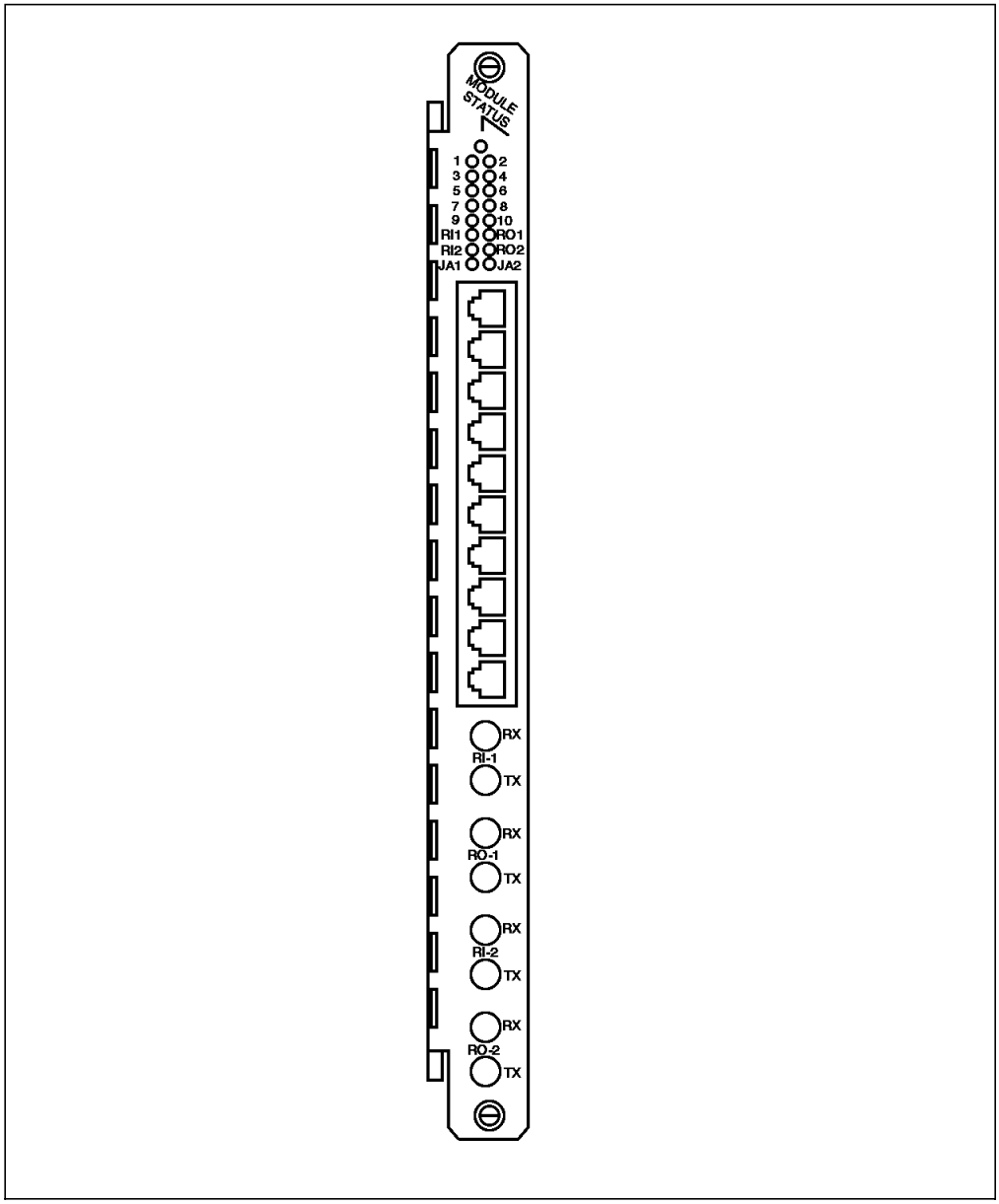


Figure 113. Front View of Dual Fiber Repeater Module

Figure 113 shows the front view of the dual fiber repeater module. As can be seen, this module provides LED indicators on the front panel that allow you to monitor the status of the module and the individual ports. Table 28 on page 176 describes the meaning of these LEDs:

Table 31 (Page 1 of 2). Dual Fiber Repeater Module LED Descriptions

LED Name	Color	State	Description
Module Status	Green	On	Module powered up OK
		Off	No Power
		Blinking	Module failed self diagnostics

Table 31 (Page 2 of 2). Dual Fiber Repeater Module LED Descriptions			
LED Name	**Color**	**State**	**Description**
RI/RO	Green	On	Trunk enabled and operating
		Off	Trunk disabled.
		Blinking	Trunk enabled but not operating normally
JA1 and JA2	Green	On	JADC card installed and operating normally
		Off	JADC card not installed
		Blinking	JADC card failed diagnostics
Port Status	Green	On	Port enabled and operating normally on the ring
		Off	Port disabled
		1 blink	Port enabled, no phantom

Figure 114 shows the side view of the dual fiber repeater module. As can be seen, in addition to the 11 isolated segments and the mounting for one T-MAC, there is an 8-position DIP switch located on the module. These DIP switches are used in the absence of an installed management module in the 8260. However, if a management module is installed in your 8260, the setting of these DIP switches will be ignored unless ″DIP_CONFIGURATION″ is enabled for DMM. For more information, please refer to 4.2.4.4, “ Configuring DMM Device” on page 50.

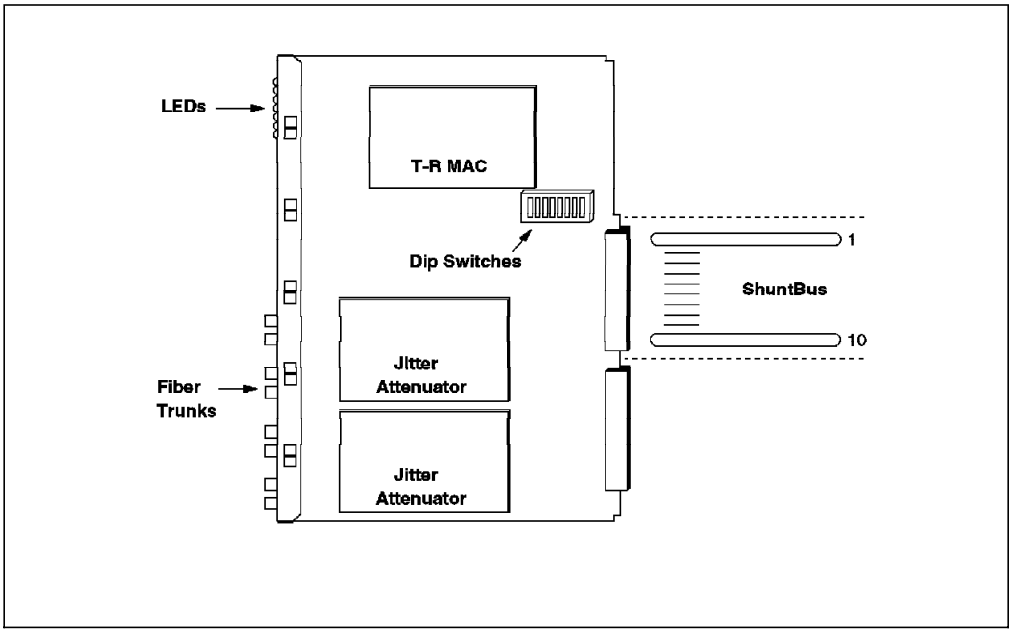


Figure 114. Dual Fiber Repeater Module Side View

The DIP switch settings on this module are identical to those of the 18-port active per-port switching module which is described in 9.3.1, “Configuring the 18-Port Active Per-Port Switching Module” on page 177.

9.6.1 Configuring the Dual Fiber Repeater Module

To configure this module you must do the following:

1. Set beacon threshold for the module.

   When a beaconing condition is detected on a lobe port, the port is wrapped by the Recovery ASIC. The port is unwrapped when a transition of phantom is detected or when the port disabled and then re-enabled by the user.

   The number of times that a phantom transition is allowed to cause a port to unwrap is determined by the *bcn_threshold* parameter which can be set for each module using the following command:

   ```
   SET MODULE {slot.port} BCN_THRESHOLD {0-255}
   ```

   Once the threshold is exceeded, the port or trunk remains wrapped until the user disables and re-enables the port. While wrapped, the port status is *BCN THRES EXCEEDED*.

   Note: The bcn_threshold is reset whenever a port successfully inserts into the ring, or the module is reset.

2. Enable/disable static switch for each lobe port.

   If you want the user of a port to power down the station before that port can be switched to another network segment, you must enable the static_switch for the specified port using the following command:

   ```
   SET PORT {slot.port} STATIC_SWITCH {enable}
   ```

   For more information about static_switch please refer to 8.6.2, “Static Switch on the Per-Port Switching Modules” on page 145.

   Note: Trunk ports can be switched between different segments at any time.

3. Assign ports to network segments.

   Use the following command to assign each port on the module to one of the backplane segments or isolated segments on the module:

   ```
   SET PORT {slot.port} NETWORK {network}
   ```

4. Assign RI/RO trunk ports to network segments.

   You can assign RI/RO trunk ports to a network using the following command:

   ```
   SET TRUNK {slot} RING_IN.n NETWORK {network} or
   SET TRUNK {slot} RING_OUT.n NETWORK {network}
   ```

   In this command ″n″ is used to specify the set of RI/RO trunks for which this command is issued. ″1″ specifies the top and ″2″ specifies the bottom set.

   Note: If you assign a RING_IN (or RING_OUT) trunk to a segment, the other trunk within that set will automatically be assigned to the same segment.

5. Set compatibility mode for the trunk ports.

   Depending on the hub to which the trunk is attached you must set the compatibility mode as described in 9.3.1, “Configuring the 18-Port Active Per-Port Switching Module” on page 177.

   To set the compatibility mode for a trunk, you can use the following command:

   ```
   SET TRUNK {slot} RING_IN.n COMPATIBILITY_MODE {mode} or
   SET TRUNK {slot} RING_OUT.n COMPATIBILITY_MODE {mode}
   ```

6. Enable/disable trunks.

Trunk ports can be enabled/disabled using the following command:

```
SET TRUNK {slot} RING_IN.n MODE {enable|disable} or
SET TRUNK {slot} RING_OUT.n MODE {enable|disable}
```

7. Enable/disable ports.

   Each port can be enabled/disabled using the following command:

   ```
   SET PORT {slot.port} mode {enable|disable}
   ```

Chapter 10. 8260 RMON Support

This chapter is intended to provide an understanding of the Remote Network Monitoring (RMON) concepts and to describe what facilities are provided by RMON to help you manage your Ethernet and token-ring LANs. These concepts are common to all RMON products though their implementation may differ.

10.1 RMON Overview

The concept of remote network monitoring (RMON) was conceived to meet the requirements for truly distributed remote network management. In RMON, the monitoring and management functions are assigned to intelligent probes distributed throughout the network. These devices, called RMON probes or RMON agents, monitor and collect traffic statistics on the network segment to which they are attached.

RMON provides a view of the data-link layer of the 802.3/Ethernet and 802.5/token-ring networks. The data-link layer, as shown in Figure 115 is just above the physical layer in the OSI stack and provides reliable delivery of data across the underlying physical network.

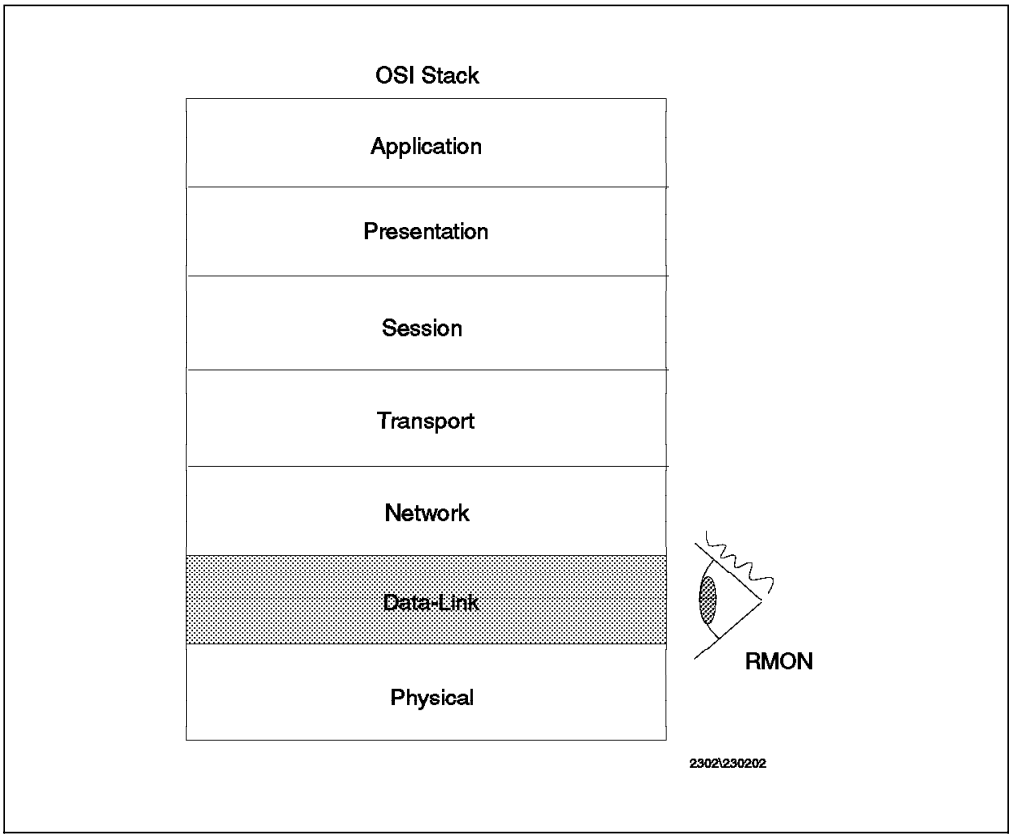


Figure 115. OSI Stack

The RMON framework is currently defined for managing 802.3/Ethernet and token-ring LAN environments. The FDDI extensions for RMON have yet to be completed. RMON provides comprehensive Ethernet and token-ring LAN network monitoring support functions such as statistics collection, threshold monitoring, historical statistics collection, problem diagnostics and report

generation. Information provided by RMON can be used for identifying sources of network problems, for fine-tuning network performance, and planning for network expansion.

RMON uses SNMP for communication between the network management station and RMON agents. Unlike SNMP devices, RMON keeps polling traffic overhead to a minimum as the RMON probes are not continuously polled.

Note

RMON provides a lot of statistical data detailing the network operations at the media level. This information, though very useful, should be used in the context of the nature of the activities occurring in the network. They should be used in assisting further investigations. For instance, when RMON reports a high packet rate and high utilization, we need to investigate further what is the nature of the traffic that caused those statistics to rise significantly. Are those data packets or non-data packets? Non-data packets require further investigation while data packets could simply result from someone performing a large file transfer.

10.1.1 Network Probes

The implementation of RMON requires network probes to be installed on each managed LAN segment throughout the enterprise network as depicted in Figure 116 on page 193. These network probes are devices whose resources are dedicated to managing the LAN segments they are attached to. Resources required by these network probes are very much dependent on the number of devices in the segment to be managed, traffic flow, type of data to be collected, frequency of collection, multiple manager requests, etc. Usually, one probe per segment is recommended for monitoring and data collection.

Network probes can be stand-alone specialized probes, integrated hub/bridge/router agents, or RMON agent software running on workstations. A subset of the RMON MIB must be present on these devices to function as an RMON agent. RMON agents can be found in bridges, routers, and hubs. Bridges and routers are not recommended as RMON agents as their primary roles are to get the traffic moving without imposing additional overhead.

10.6, “Monitoring Functions Supported In 8260” on page 212 discusses the RMON agents implemented in the 8260 DMM (along with T-MAC and E-MAC daughter cards).

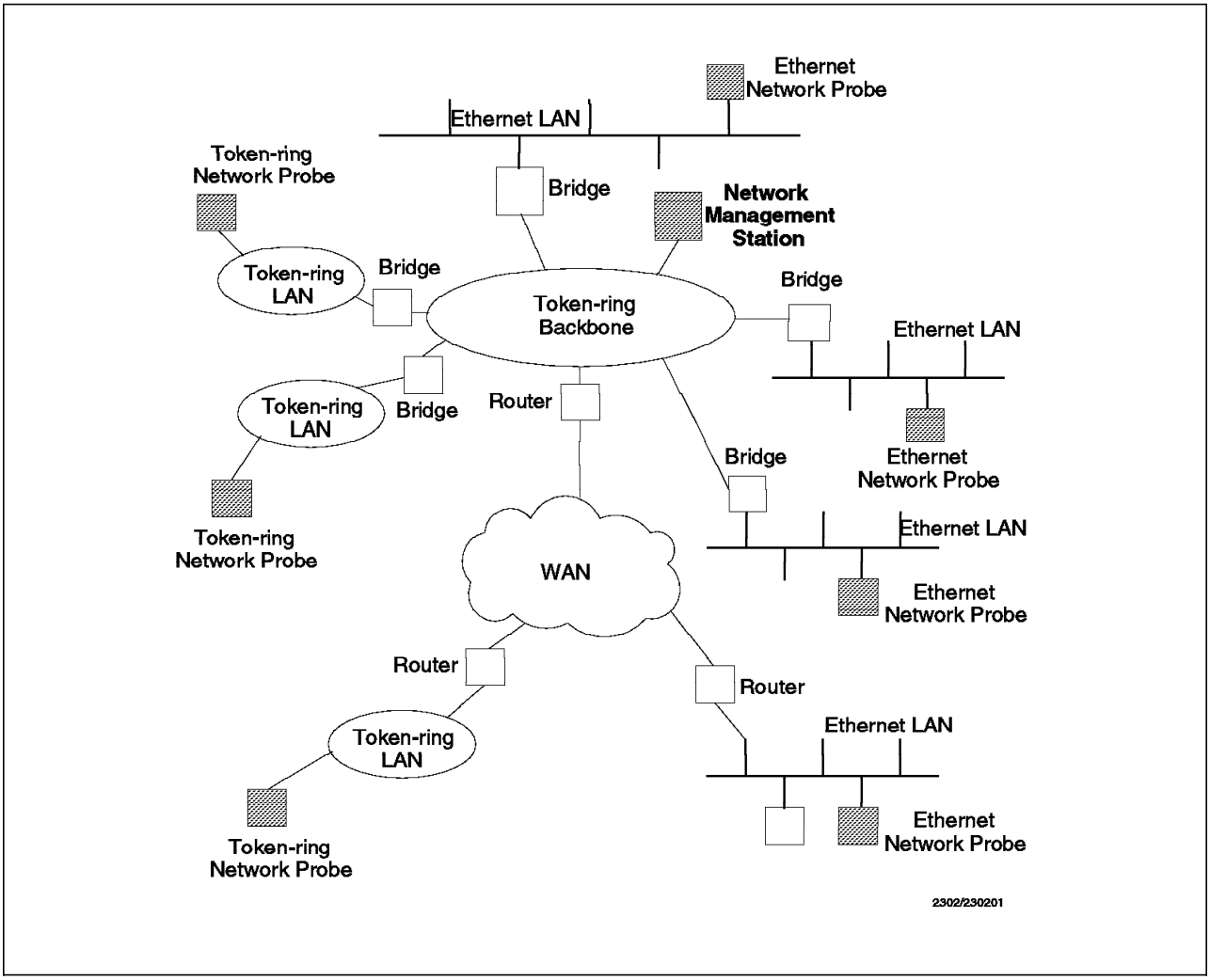


Figure 116. An Example of RMON Implementation

10.1.2 RMON Manager

The network management station, also known as the RMON manager, works in conjunction with the RMON agents to provide a central point for managing and consolidating information gathered by the RMON agents. To minimize network overhead, the RMON manager does not continuously poll the agents although it has the ability to do so. The information collected by individual agents is transferred to the RMON manager at specified time intervals. The transfer can be arranged to take place during off-peak hours. In addition, the RMON manager can request the information to be transferred on demand.

Each agent can be configured by the RMON manager to monitor and collect LAN statistics at specified time intervals for the desired duration, and to forward the information gathered at a specified frequency. Alarms can be configured on the agents to generate events that inform the manager of a certain threshold incident. This eliminates the need for the manager to constantly poll the RMON agents, thus reducing network traffic overheads.

From the information provided by the RMON agents, the RMON manager can get a ″bird′s eye″ view of the current state of the entire network at a glance. The information can be used to pro-actively manage the network by monitoring

baseline network characteristics, quickly spotting potential trouble spots and resolving them before major crises occur.

10.2 RMON Goals

To ensure that RMON can function effectively and efficiently in a distributed environment, its framework was designed with the following goals:

- Offline operation
- Preemptive monitoring
- Problem detection and reporting
- Value-added data
- Multiple managers

10.2.1 Offline Operation

The offline operation prevents the remote network monitoring functions from being crippled due to network failures or lost communications with the management station. Fault, performance and configuration information will be accumulated continuously on the network probe when communication with the management station is not possible or efficient. When an exception condition occurs, the probe will attempt to notify the management station.

In wide area network (WAN) environments or when dial-up links are used, this feature can help reduce communications costs.

10.2.2 Preemptive Monitoring

Preemptive monitoring provides for historical statistical information to be collected and stored. Historical information captures trends, related events and information that can allow one to witness the occurrence of the problem. By playing back the historical information collected, a detailed diagnosis can be performed to ascertain the cause of a problem.

10.2.3 Problem Detection and Reporting

The RMON agent is fully responsible for problem detection and reporting on the segment that it manages. It can be configured to detect specific conditions such as error conditions and continuously monitor their occurrence. When a problem is detected, the RMON agent is configured to take the necessary action such as logging the event and raising an alert to the RMON manager.

10.2.4 Value Added Data

Statistics are important for problem determination. Occasionally, statistics don't portray the complete scenario for a detailed diagnosis to be performed on the problem. Since the RMON agents are directly monitoring the LAN segments, they intimately know what happens in the segments. As such, they are able to add significant value to the data being collected. For example, we can know who is causing the network utilization to rise above the threshold level, if the probe can highlight the hosts that generate the most traffic.

10.2.5 Multiple Managers

The RMON framework permits the RMON agents to be managed by multiple network management stations concurrently. This is useful for implementing disaster recovery, and allowing different units or functions in the organization to access information provided by the RMON agents. For instance, the network planning group may want to continuously track the bandwidth utilization of each segment for capacity planning. Elsewhere help desk personnel are trying to figure out which interface adapter is transmitting error packets.

10.3 Standards

The RMON MIB has been ratified as a new subset of standards for SNMP.

- RFC 1271 Remote Network Monitoring (RMON) MIB for Ethernet
- RFC 1513 token-ring extensions to the RMON MIB

IBM employees can retrieve the RFC documents from VM/CMS by typing:

```
tools sendto almvma arcnet rfc get rfcxxxx  txt
```

The *rfcxxxx* can be rfc1513 or rfc1271.

IBM customers may request the documents from their IBM marketing representatives.

The RMON MIBs (RFC 1271 and RFC 1513) should be considered the basic documentation for RMON products.

10.4 Managing the Ethernet LAN Environment

The RMON MIB for Ethernet contains specific statistics for managing the Ethernet LAN environment. A proper understanding of Ethernet LAN architecture is required to fully appreciate what each statistic means and how it is calculated. 7.1, “Ethernet LAN Overview” on page 97 provides a brief description of the Ethernet LAN environment characteristics. For further information about the Ethernet LAN architecture, please refer to *LAN Concepts and Products,* GG24-3178.

10.4.1 Managing Ethernet LANs with RMON

Network probes for Ethernet must implement the remote monitoring functions based on the framework as defined in the RFC 1271 RMON MIB specifications. This MIB defines objects which are divided into nine different functional groups as summarized in Table 32 on page 196.

This RFC defines many objects suitable for the management of multiple network types and contains some objects defined specifically to give a view of the data-link layer for Ethernet media.

The purpose of the following sections is to help you understand what each of the RMON statistics is and how it is calculated.

Table 32. MIB Structure for RFC 1271 - RMON MIB for Ethernet	
Group	**Description**
Statistics	The Statistics group provides an overview of the current segment network activity at any given moment. It collects segment statistics like octets, packets, collisions, broadcast, various error counters and packet size.
History	The History group records periodic statistical samples from a segment and stores them for later retrieval.
Alarm	The Alarm group periodically takes statistical samples from variables in the RMON agent and compares them to defined thresholds. When a threshold is crossed, an event will be generated. It is useful to track unusual activity or problems.
Host	The Host group maintains host tables by keeping a list of source and destination MAC addresses seen in good packets. In addition, statistics like octets and packets transmitted and received, errors transmitted, broadcast and multicast packets are kept on a per host basis. In problem determination, it is extremely useful for isolating the culprit by its interface address that, for instance, is causing the error count to rise sharply.
Host Top ″N″	The Host Top ″N″ group provides lists of a given number of hosts that meet a particular criteria ordered by one of their statistics. For instance, you can list the top 5 packet sending hosts. This helps in isolating the hosts that are creating network problems.
Matrix	The Matrix group monitors and stores information about conversations between two hosts in the network.
Filter	The Filter group allows packets of particular interest to be filtered and isolated. These packets can then be directed into capture buffers or used to trigger events. It is useful for monitoring traffic flow and setting alarm conditions.
Packet Capture	The Packet Capture group allows packets to be captured upon a filter match and stored for later retrieval. It can be used to view the history of packet activity in the event of a failure.
Event	The Event group controls the generation and notification of events from the RMON agent. It contains a log table that associates logged entries with a specific event.

10.4.1.1 Statistics Group

The Statistics group contains very useful statistical information gathered by the network probe through its Ethernet interface. The information provided by this group gives a view of the total Ethernet LAN segment activity at any given moment. It samples data and provides information by octets, packets, various error counters and packet size. The statistics take the form of free running counters that start from zero. Here is the list of statistics available under this group:

Drop Events The number of events in which packets were dropped by the probe due to unavailability of resources on the probe itself. It doesn′t represent the number of packets dropped but the number of times this condition was detected. If the drop events counter constantly increments, it is an indication that there is more activity on the segment than can be captured by the network probe. You may want to consider increasing the resources on your network probe. For instance, if you are running the RMON application on a workstation, you may want to allocate more real

memory and disk space to the RMON application. If you are running RMON subset on a bridge or router, you might want to consider offloading the task to an external monitoring device.

Octets The number of octets of data (including those in bad packets) received on the network (including the FCS octets but excluding the framing bits). The term ″octet″ is used to refer to 8 bits. The term ″byte″ is not used because some devices have byte sizes greater than 8 bits.

Packets The number of packets received on the segment. Frame and packet are synonymous in this context. This includes good as well as error packets received.

Broadcast Packets The number of good packets received that were directed to the broadcast address. A broadcast is a message that you want every station on the network to see. Broadcasts are normal in all networks. Broadcasts are widely used in most LAN protocols to distribute information to all hosts in the network. Incorrect device configuration, application errors, or protocol problems can create broadcast storms, where broadcast packets are continuously transmitted throughout the network or in large spikes. Broadcast storms can greatly degrade the performance of a network.

Multicast Packets The number of packets received that were directed to a multicast address. Multicast packets are more commonly found in DECnet environments where they are used for communicating with end nodes and routers. This does not include packets directed to broadcast addresses.

CRC Align Error The number of corrupted packets received that had a length of between 64 and 1518 octets (excluding the framing bits, but including the FCS octets), and inclusive of the following:

- Not an integral number of octets in length
- Bad Frame Check Sequence (FCS)

Undersized Packets A legal Ethernet packet size ranges from a minimum of 64 octets to a maximum of 1518 octets in length (excluding framing bits but including FCS octets). An Undersized packet is one whose length is less than 64 octets but was otherwise well formed. The term ″runt″ refers to an undersized packet.

Oversized Packets An Oversized packet is one whose length is more than 1518 octets (excluding framing bits, but including FCS octets) but was otherwise well formed.

Jabbers Jabbers are similar to CRC Align Error packets with the exception that each jabber packet is more than 1518 octets in length. These errors may indicate that your network needs to be fine-tuned, or network buffers are insufficiently configured, etc.

Fragments Fragments are similar to CRC Align Error packets with the exception that each fragmented packet is less than 64 octets in length. This can indicate a high collision rate.

Collisions The number of collisions detected on the network. Collisions are common phenomena on Ethernet segments. Excessive collisions are detrimental to network performance. It is an indication that you have too many stations trying to communicate simultaneously. If the situation persists, perhaps it's time to consider further segmenting of your network.

Packet Size Statistics The probe keeps individual counters for the occurrences of packets with the following lengths:

- 64 octets
- 65-127 octets
- 128-255 octets
- 256-511 octets
- 512-1023 octets
- 1024-1518 octets

10.4.1.2 History Group

The History group provides a means of correlating the data gathered by the Statistics MIB over time. It records statistical samples according to a user-specified time interval and duration and stores them for later retrieval.

The History MIB can be used to gather separate studies collected simultaneously from various probes and at different intervals. For instance, you can set up a session to collect statistical data via the Statistics MIB from several probes every 10 seconds for real-time monitoring. The History MIB can be configured to gather statistics from the same sources at intervals of 30 seconds for an ongoing portrait, and at 30-minute intervals for later study.

You are encouraged to set up two history control entries per monitored interface upon initialization. One can be set for short term polling at intervals of 30 seconds and another for long term polling at 30 minute intervals.

Each interval saved is referred to as a "bucket". The number of buckets to be used is defined by the operator. The interval can range from one second to one hour.

Note

It is important to configure the appropriate time interval for data sampling as no indication will be given when the statistical counters overflow their maximum value. For instance, on a heavily-loaded Ethernet segment, the *etherHistoryOctets* counter could overflow in about an hour. Following this, the information stored by this counter will not reflect the true state as it will reset to zero and start incrementing again. The maximum counter value of the RMON agent varies according to implementation and hardware architecture. On the RMONitor Agent for OS/2 device, the maximum counter value is 2^{32}.

The History Control table stores configuration entries containing the interface information, polling period, number of buckets requested, and number of buckets granted. The number of buckets requested represents the number of times the operator wants to collect and store the samples. The probe will respond with the number of buckets granted based on the requests as well as available resources.

At each sampling cycle, the following statistics are collected and stored:

- Drop events
- Octets
- Packets
- Broadcast packets
- Multicast packets
- CRC align error packets
- Undersized packets
- Oversized packets
- Fragments
- Jabbers
- Collisions
- Utilization

All of the above are also gathered by the Statistics MIB with the exception of utilization. For an explanation of the individual statistics, please refer to 10.4.1.1, “Statistics Group” on page 196.

The utilization statistics give the Ethernet physical layer network utilization during the specified time interval, in hundredths of a percent.

10.4.1.3 Alarm Group

The Alarm group is used to track extraordinary activities or events. It permits the operator to set the RMON alarms to specific thresholds, and when traffic exceeds or drops below those thresholds, an event is activated. Thresholds can be defined as a rising threshold or a falling threshold.

A rising threshold is used to monitor the value of a tracked variable when it rises above a particular level. For instance, you might want to set a rising threshold for the occurrences of error packets at 200 packets/second. If the error packet rate exceeds 200 packets/sec, the rising threshold is exceeded and an event will be generated.

A falling threshold is used to report an event when the value of a tracked variable has fallen below a particular threshold level.

Thresholds can be set against either absolute or delta values. If an absolute value is chosen, the absolute value stored in the variable′s counter will be compared directly with the absolute threshold value. For delta values, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the threshold value.

10.4.1.4 Host Group

The Host group creates and maintains a host table for the segment monitored. The Host MIB is very useful as it contains information and cumulative statistics for every discovered host such as:

- Host MAC address
- Good packets/octets received/transmitted
- Error packets transmitted
- Broadcast packets transmitted
- Multicast packets transmitted

The information provided by the Host MIB is stored for each MAC host. If the error count or broadcast count rises sharply, it is relatively easy to isolate the culprit by host address.

Note: As this process consumes a lot of storage, the monitoring device may delete entries as needed based on the least recently used (LRU) entries first.

10.4.1.5 Host Top N Group

The Host Top N group provides a list of a given number of hosts that are top-performers based on selected statistics. The user can select statistics from the base Statistics MIB, taken over an interval period specified by the management station. The number of such hosts to be selected is also specified by the management station.

For instance, you can specify viewing the top 5 senders, top 10 broadcast hosts, top 3 multicast hosts, etc. The Host Top N group can be particularly useful in isolating hosts that are a source of problems in the network.

10.4.1.6 Matrix Group

The Matrix group consists of tables that store statistics for a particular conversation between two addresses. New entries are appended as the monitoring device detects new conversations.

Three tables are maintained within the Matrix group:

- Control table
- Source-Destination table
- Destination-Source table

The Control table specifies the maximum number of entries to be captured and placed into the Source-Destination table and Destination-Source table. As more and more conversations are appended, resources will be recovered by deleting the least recently used entries.

The Source-Destination table captures statistical information about a conversation between two hosts and indexes that information from a transmitter-oriented perspective.

The following information is stored in this table:

- Source MAC address
- Destination MAC address
- Number of packets transmitted (including error packets)
- Number of octets transmitted
- Number of errors transmitted

The Destination-Source table captures similar information but indexes it from a receiver-oriented perspective.

10.4.1.7 Filter Group

The Filter group allows packets that are of particular interest to be captured using arbitrary filter expressions. These packets are then directed into channels that can be turned on or off to control the packet flow.

The channels can also generate events when the packets are passing through them.

The Filter group provides the administrator with the flexibility of monitoring traffic flow as well as setting alarm conditions.

10.4.1.8 Packet Capture Group

The Packet Capture group allows packets to be captured after they flow through a channel. Packets may be flowing through different channels and a number of active capture buckets can be active concurrently. Each buffer can be set either to stop collecting data when full, or to wrap around when it is full. Packet Capture allows the administrator to have a historical view of the packet activity in the event of a failure.

10.4.1.9 Events Group

The Events group controls the generation and notification of events from the monitoring device. Events can be triggered when traffic triggers alarms as well as from traffic flowing through preset channels. The events, in turn can trigger some other actions such as creating a log entry or initiating an SNMP trap or turning a channel on or off.

The Events group maintains the following two tables:

- An Event table that contains events that can be generated when certain conditions are met.
- A Log table to log generated events.

10.5 Managing the Token-Ring LAN Environment

Managing the token-ring environment as with Ethernet, requires knowledge and understanding about its architecture. The token-ring extension for the RMON MIB presents a view of the data-link layer of a token-ring LAN. 8.1, “Token-Ring LAN Overview” on page 129 provides a breif description of the token-ring architecture and terminologies used in the token-ring LAN environment. For detailed information, please refer to *Token-Ring Network Architecture Reference,* SC30-3374 and *Local Area Network Concepts and Products,* GG24-3178.

10.5.1 Managing Token-Ring LANs with RMON

RFC 1513 was created as an extension to the RFC 1271 RMON MIB to include definitions for specific objects as well as some additional monitoring functions necessary for token-ring LANs. Some groups within the RFC 1513 MIB structure require the implementation of certain groups found in RFC 1271. For more details please refer to RFC 1271 and RFC 1513.

Table 33. MIB Structure for RFC 1513 - Token-Ring Extensions to the RMON MIB		
Group		**Description**
Token-ring Statistics	Token-ring MAC-layer Statistics	This group collects ring error statistics and ring utilization from the MAC layer. It samples MAC data and provides information like MAC octets, MAC packets, beacon packets, line errors, burst errors, token errors, lost frame errors, congestion errors, etc.
	Token-ring Promiscuous Statistics	This group collects statistics from non-MAC packets collected like data packets, broadcast packets, multicast packets, etc.
History	Token-ring MAC-layer History	This group contains historical utilization and error statistics collected from the MAC-layer.
	Token-ring Promiscuous History	This group contains historical utilization and error statistics collected from data packets.
Ring Station		This group contains statistics and status information associated with each token-ring station on the local ring. Information provided includes number of active stations, current status of ring, active monitor, etc.
Ring Station Order		This group provides the order of the stations on monitored rings.
Ring Station Configuration		This group can manage the token-ring stations through active means. It can download configuration information as well as remove any station on a monitored ring.
Source Routing		This group collects utilization statistics derived from source routing information present in token-ring packets in a source route bridging environment.

10.5.1.1 Statistics Group

The Statistics group provides a real-time view of the token-ring segment activity as measured by the network probe attached to that segment. The statistics take the form of free running counters that start from zero.

The Statistics group is divided into *MAC-Layer* and *Promiscuous* subgroups. The MAC layer sits between the 802.2 LLC interface and the physical hardware. MAC packets provide information that describes the physical condition of the LAN.

Note

Promiscuous simply refers to non-MAC related objects such as data packets, broadcast packets, multicast packets, etc. These packets must be collected ″promiscuously″. In other words, the device driver of the adapter must be enabled to deliberately pick up those packets and pass them along to the higher layers.

The Token-Ring MAC-Layer Statistics Group: The MAC-layer statistics group collects ring error statistics and ring utilization from the MAC layer. This group samples MAC data and provides information like MAC octets, MAC packets, beacon packets, line errors, burst errors, token errors, lost frame errors, congestion errors, etc.

Here is a list of MAC statistics available under this group and their respective descriptions:

Drop Event

The number of events in which MAC packets were dropped by the probe due to unavailability of resources on the probe itself. It doesn't represent the number of packets dropped but the number of times this condition was detected. If the drop events counter constantly increments, it is an indication that there is more activity on the segment than can be captured by the network probe. You may want to consider increasing the resources on your network probe. For instance, if you are running the RMON application on a workstation, you may want to allocate more real memory and disk space to the RMON application. If you are running an RMON subset on a bridge, router, or hub, you might want to consider offloading the task to an external monitoring device.

MAC Octet

The number of octets of data in MAC packets (excluding bad frames) received on the network (including the FCS octets but excluding the framing bits). An octet represents an integral collection of eight bits of information.

MAC Packet

The number of MAC packets received. This excludes packets that were not good frames.

Ring Purge Event

A ring purge event refers to one of the following occurrences:

- Completion of the token-claiming process
- Detection of a token error such as a lost frame or token, a circulating frame, or a circulating priority token

The probe will count the number of times the ring enters the ring purge state from normal ring state. It doesn't include a ring purge state that comes in response to the claim token or beacon state.

Errors caused by adapter insert/removal can also trigger a ring purge. Adapter insert/removal operations are normally encountered in the morning when employees power-on their PCs to access the LAN and when they power-off their PCs in the evening. A baseline should be set to ignore high counts of ring purges during hours when PCs are being powered-on/off.

Ring Purge Packet

A Ring Purge MAC frame/packet is sent by the active monitor to all ring stations informing them about the occurrence of a ring purge event.

Beacon Event

This counter keeps track of beacon events. A beacon event occurs when the ring enters the beaconing state from a non-beaconing state. A beaconing state could result from:

- Ring signal loss error

- Recovery mode set
- Streaming signal (not Claim Token MAC frame)
- Streaming signal, Claim Token MAC frame or intermediate detection of hard error

Beacon Time — Keeps track of the amount of time that the ring has been in the beaconing state.

Beacon Packet — Refers to the total number of Beacon MAC frames detected by the probe.

Claim Token Event — This counter keeps track of the total number of claim token events detected by the probe. A claim token event occurs when the ring enters the claim token state from normal ring state or ring purge state. The claim token state that comes in response to a beacon state is not included. The claim token event occurs when:

- The active monitor detects a loss of signal, detects expiration of its receive_notification timer, or cannot receive enough of its own Ring Purge MAC frames.
- The standby monitor detects a loss of signal, or detects expiration of its good_token or receive_notification timers.
- A ring station attaches to the ring and does not detect an active monitor.

Claim Token Packet — Refers to the total number of Claim Token MAC frames detected by the probe.

NAUN Change — Any ring station upon detecting a change in the address of its nearest active upstream neighbor (NAUN) during the neighbor notification process will send a NAUN Change MAC frame to the configuration report server. This address change indicates that either a ring station has attached to the ring, or a station has removed itself from the ring.

Line Error — This error counter is incremented when the ring station detects:

- A code violation between the starting and ending delimiters of the frame or token
- A Frame Check Sequence error

Line errors will increment the error counters for the station reporting the problem and its nearest upstream neighbor. This error is reported in the Soft Error Report MAC frame.

Internal Error — This error is flagged when a ring station is detected to be in a marginal operating condition. This statistic is found in the total number of internal errors reported in the Soft Error Report MAC frame.

Burst Error — This error occurs when a new station is inserted into the ring. It is normally reported by downstream stations and occurs more frequently on a 16 Mbps LAN than a 4 Mbps LAN. This statistic is found in the

total number of burst errors reported in the Soft Error Report MAC frame.

ACErrors

This error is flagged when a frame is copied by an adapter to which it was not addressed. Address Copied Errors or ACErrors will increment the error counter only for the nearest upstream neighbor of the station reporting the error. This statistic is found in the total number of ACErrors reported in the Soft Error Report MAC frame.

Abort Error

This keeps track of the number of times a ring station transmits an abort delimiter to abort a frame it transmitted. This statistic is found in the total number of Abort errors reported in the Soft Error Report MAC frame.

Lost Frame Error

Represents how often frames transmitted by a particular ring station fail to return to it and thus the active monitor has to issue a new token. This statistic is found in the total number of Lost Frame errors reported in the Soft Error Report MAC frame.

Congestion Error

Occurs when a station cannot copy the frame addressed to it due to lack of receive buffers on the adapter. This is commonly referred to as *Receiver Congestion.* Sometimes the problem may not actually be in the receiving station, but in one or more stations sending excessive number of frames to the congested adapter. This statistic is found in the total number of Congestion errors reported in the Soft Error Report MAC frame.

Frame-Copied Error

The Frame Copied Soft error counter is incremented each time a destination station sees a frame addressed to it and the Address Recognized and Frame Copied bits set on. Under normal conditions this would indicate a duplicate address in the network, since stations would turn on those bits when they recognize a frame addressed to them and can copy it. However, with bridges the scenario is changed. As a bridge sees a frame that it must copy, it marks the AC/AC bits on the Frame Status field on the local ring. When the frame is placed on the remote ring those fields are cleared. Therefore on a ring with bridges it is not uncommon to see many Frame Copied soft errors. Also, be aware that the Frame Status field is the only type of frame checked to verify that the frame has successfully reached its destination. LLC frames depend on several timers (T1/T2/Ti) to do link-level acknowledgments and even though the Frame Status field is updated, it will not be checked at the adapter level.

This statistic is found in the total number of Frame Copied errors reported in the Soft Error Report MAC frame.

Frequency Error Occurs when a ring station detects a frequency error. A new station inserting into the ring can cause downstream stations to be ″off frequency″. This condition seems to happen more on 16 Mbps than 4 Mbps rings. This statistic is found in the total number of Frequency errors reported in the Soft Error Report MAC frame.

Token Error Token errors occur when a token is destroyed or corrupted. This usually occurs when devices insert or remove themselves from the ring. This statistic is found in the total number of token errors reported in the Soft Error Report MAC frame.

Soft Error Report The Soft Error Report contains a compilation of all soft errors detected by a ring station. At every two-second interval, each ring station will transmit a Soft Error Report MAC frame to the ring error monitor if the counters are greater than zero. This enables the ring error monitor to maintain accurate error statistics. A soft error refers to an intermittent network error that causes data to be retransmitted. If the number of soft errors becomes excessive, network reliability and performance can be seriously impacted.

Ring Poll Event A Ring Poll event is triggered by the occurrence of an *Active Monitor Present MAC frame*. It is initiated by the active monitor to all ring stations to:

- Inform standby monitors of the active monitor′s presence
- Indicate that the ring is functioning correctly
- Initiate a neighbor notification (NAUN)

The Token-Ring Promiscuous Statistics Group: This group gathers current utilization statistics from non-MAC packets on a particular token-ring interface. The statistics like data packets, data octets, broadcast packets, multicast packets, packet size, etc., are collected promiscuously. In other words, the device driver for the token-ring adapter must be enabled to deliberately copy all non-MAC packets even though they are not addressed to it.

Here is a list of statistics available under this group and their respective descriptions:

Drop Event The number of events in which non-MAC packets were dropped by the probe due to unavailability of resources on the probe itself. It doesn′t represent the number of packets dropped but the number of times this condition was detected. If the drop events counter constantly increments, it is an indication that there is more activity on the segment than can be captured by the network probe. You may want to consider increasing the resources on your network probe. For instance, if you are running the RMON application on a workstation, you may want to allocate more real memory and disk space to the RMON application. If you are running an RMON subset on a bridge, router,

or hub, you might want to consider offloading the task to an external monitoring device.

Octets

The total number of octets of data in good frames received on the network in non-MAC packets (including the FCS octets but excluding the framing bits). An octet represents an integral collection of eight bits of information.

Packets

The total number of non-MAC packets in good frames received on the network.

Broadcast Packets

The total number of good non-MAC frames received that were directed to an LLC broadcast address (0xFFFFFFFFFFFF or 0xC000FFFFFFFF). Broadcasts are normal in all networks. For example, when an X-terminal is powered up, it generates some broadcast packets to locate the server station. Excessive broadcasts, known as broadcast storms, can greatly deteriorate network performance.

Multicast Packets

The total number of good non-MAC frames received that were directed to a local or global multicast or functional address. This does not include packets directed to the broadcast addresses.

Packet Size Statistics

The probe keeps individual counters for counting the number of frames detected with the following frame lengths:

- 18-63 octets
- 64-127 octets
- 128-255 octets
- 256-511 octets
- 512-1023 octets
- 1024-2047 octets
- 2048-4095 octets
- 4096-8191 octets
- 8192-18000 octets
- Greater than 18000 octets

This information can be used to fine-tune your network buffers to accommodate the appropriate traffic loads. It can also be used to determine what packet sizes are commonly used. Some applications can be modified to use a different frame size. This can help in tuning the network.

You can also use this information for acquiring bridges, routers, and hubs that are better suited for your network environment. Bridges or routers or hubs offer varying performance throughputs based on different packet sizes. Some of this equipment works well with large packet sizes while others don′t. So armed with the knowledge of what packet sizes occupy your network, you can make a better purchase decision.

10.5.1.2 History Group

The token-ring History groups capture historical information about network utilization and error statistics for the token-ring network. They provide a means of correlating the data collected by the Statistics group over time. They record statistical samples according to a user-specified frequency and duration and store them for later retrieval.

The History MIB can be used to gather separate studies collected simultaneously from various probes and at different intervals. For instance, you can set up a session to collect statistical data via the Statistics MIB from several probes every 10 seconds for real-time monitoring. The History MIB can be configured to gather statistics from the same sources at intervals of 30 seconds for an ongoing portrait, and at 30-minute intervals for later study.

It is advisable to set up two history control entries per monitored interface upon initialization. They can be a combination of short term polling at 30-second intervals and long term polling at 30-minute intervals.

Each interval saved is referred to as a ″bucket″. The number of buckets to be used is defined by the operator. The intervals over which the data is sampled for each bucket can be set to any number of seconds from one to 3600 (one hour).

Note

It is important to configure the appropriate time interval for sampling the statistical data as no indication will be given when the statistical counters overflow their maximum value. For instance, on a heavily-loaded token-ring segment, the *tokenRingMLHistoryMacOctets* counter could overflow in a short time. Following this, the information stored in this counter will not reflect a correct value. Once the maximum value is reached it will reset to zero and begin incrementing again.

The History groups are broken down into two sub-groups (similar to the token-ring Statistics groups):

- MAC-Layer History group
- Promiscuous History group

MAC-Layer History Group: The token-ring MAC-Layer History group will collect and store the MAC-layer statistics based on user-defined frequency and duration. This group contains a total of 24 different counters for collecting and storing the following MAC-layer statistics:

- Drop Events
- Mac Octets
- Mac Packets
- Ring Purge Events
- Ring Purge Packets
- Beacon Events
- Beacon Time
- Beacon Packets
- Claim Token Events
- Claim Token Packets
- NAUN Changes

- Line Errors
- Internal Errors
- Burst Errors
- Address Copied Errors
- Abort Errors
- Lost Frame Errors
- Congestion Errors
- Frame Copied Errors
- Frequency Errors
- Token Errors
- Soft Error Reports
- Ring Poll Events
- Active Stations

All of the above statistics are also sampled by the token-ring MAC-layer Statistics group with the exception of the Active Stations statistic. For information about the individual statistics, please refer to 10.5.1.1, “Statistics Group” on page 202.

The Active Stations statistic keeps track of the total number of active stations on the ring detected by the probe during the sampling cycle.

Promiscuous History Group: The token-ring Promiscuous History group collects and stores the promiscuous token-ring statistics based on user-defined frequency and duration. This group contains a total of 15 different counters for collecting and storing the following statistics:

- Drop Events
- Data Octets
- Data Packets
- Broadcast Packets
- Multicast Packets
- Good non-MAC frames with lengths between:
  - 18-63 octets
  - 64-127 octets
  - 128-255 octets
  - 256-511 octets
  - 512-1023 octets
  - 1024-2047 octets
  - 2048-4095 octets
  - 4096-8191 octets
  - 8192-18000 octets
  - Greater than 18000 octets

10.5.1.3 Ring Station Group

The token-ring Ring Station group maintains status information and statistics associated with each active station in the local ring. In addition, this group provides status information for each ring being monitored.

Two tables are maintained by this group:

- *RingStationControlTable*
- *RingStationTable*

The *RingStationControlTable* provides the following status information about the local ring:

- Number of active stations on the ring
- Current status of the ring with the following possible ring states:
  - Normal operation
  - Ring Purge state
  - Claim Token state
  - Beacon Frame Streaming state
  - Beacon Bit Streaming state
  - Beacon Ring Signal Loss state
  - Set Recovery Mode state
- Address of the last beacon sender
- Address of the last beacon sender's NAUN
- Address of the Active Monitor on the segment
- List of all stations currently or previously detected to be physically present on this segment

The *RingStationTable* stores status information and statistics of individual stations detected to be physically present on the local ring. For each station, the following information is stored in the *RingStationTable*:

- Station MAC address
- Its last NAUN
- Current station state (active, inactive, forced removal)
- Last ring enter time
- Last ring exit time
- Total *Duplicate Address errors* reported by the station
- Total *Line errors* reported by the station
- Total *Line errors* reported by the station's NAUN
- Total *Internal errors* reported by the station
- Total *Burst errors* reported by the station
- Total *Burst errors* reported by the station's NAUN
- Total *Address Copied errors* reported by the station's NAUN
- Total *Abort errors* reported by the station
- Total *Lost Frame errors* reported by the station
- Total *Congestion errors* reported by the station
- Total *Frame Copied errors* reported by the station
- Total *Frequency errors* reported by the station
- Total *Token errors* reported by the station
- Total *Beacon errors* reported by the station
- Total *Beacon errors* reported by the station's NAUN
- Ring insertion attempts by the station

10.5.1.4 Ring Station Order Group

The token-ring Ring Station Order group maintains a table that lists the ring stations ordered according to the ring poll with respect to the RMON probe. The location of each station is denoted by an index. With the RMON probe assigned an index of one, indexes for other stations are assigned depending on how many stations downstream they are from the RMON probe.

The station's MAC address is stored together with its index in the table. This table can be used as a quick cross-reference for locating stations based on the way they are ordered.

10.5.1.5 Ring Station Configuration Group

The token-ring Ring Station Config group provides the capability to actively manage and query the configuration of each token-ring node in the local ring.

The RMON probe can initiate the removal of a station from the ring by sending a *Remove Station MAC frame.* It keeps the following configuration parameters of each station:

- MAC address
- Microcode EC level
- Group address
- Functional address

10.5.1.6 Source Routing Group

The information collected by the token-ring Source Routing group is only applicable to the source-route bridging environment. The source routing information is present in all token-ring packets in this environment.

Do not use the information provided by this group if you are using transparent bridging or a mixed bridging/routing environment as it might not be accurate.

The token-ring Source Routing group is a collection of source routing statistics kept for a particular token-ring interface. The following statistics are collected:

In Frames Contains the count of frames sent into this ring from another ring.

In Octets Contains the count of octets in good frames sent into this ring from another ring.

Out Frames Contains the count of frames sent from this ring to another ring.

Out Octets Contains the count of octets in good frames sent from this ring to another ring.

Through Frames Contains the count of frames sent from another ring through this ring, to another ring.

Through Octets Contains the count of octets in good frames sent from another ring through this ring, to another ring.

All-Routes Broadcast Frames Contains the total number of good frames received that were All-Routes broadcast.

All-Routes Broadcast Octets Contains the total number of octets in good frames received that were All-Routes broadcast.

Single-Route Broadcast Frames Contains the total number of good frames received that were single-route broadcast.

Single-Route Broadcast Octets Contains the total number of octets in good frames received that were single-route broadcast.

Local LLC Frames Contains the total number of frames received that had no Routing Information Field (RIF) or had a RIF that only included the local ring number and were not all-routes broadcast frames. RIF contains route information provided by the Bridge Program used in the

source routing bridges. Transparent bridges do not use this field.

One-Hop Frames — Contains the total number of frames received whose route had one hop, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Two-Hop Frames — Contains the total number of frames received whose route had two hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Three-Hop Frames — Contains the total number of frames received whose route had three hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Four-Hop Frames — Contains the total number of frames received whose route had four hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Five-Hop Frames — Contains the total number of frames received whose route had five hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Six-Hop Frames — Contains the total number of frames received whose route had six hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Seven-Hop Frames — Contains the total number of frames received whose route had seven hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

Eight-Hop Frames — Contains the total number of frames received whose route had eight hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

More than 8-Hop Frames — Contains the total number of frames received whose route had more than eight hops, were not all-routes broadcast frames, and whose source or destination address were on this ring.

10.6 Monitoring Functions Supported In 8260

As mentioned in Chapter 4, “8260 Distributed Management Architecture” on page 35, the DMM uses the facilities provided by the T-MAC and E-MAC daughter cards to interface to the backplane segments. This allows DMM to use the services of T-MAC and E-MAC to monitor the network segments to which the T-MAC or E-MAC is assigned and collect various statistical information about the segment and the stations attached to these segments.

To monitor each backplane or isolated segment, a T-MAC (for token-ring segments) or E-MAC (for Ethernet segments) is required. You can use the

following command to display the status of the DMM network interfaces via T-MACs and E-MACs installed in your hub:

```
8260A> show interface
```

Figure 117 shows an example of the output from this command:

```
8260A> show interface

                      Admin Oper  MAC
Idx Network       Type Stat  Stat  Address           Slot  General Information
--- ------------- ---- ----- ----- ----------------- ----- -------------------

  2 SLIP          SLIP DOWN  DOWN  N/A               N/A
  3 ETHERNET_1    ETH  UP    UP    10-00-f1-0c-68-3a 01.02
  4 ETHERNET_3    ETH  UP    UP    10-00-f1-0c-c0-f7 02.02
  5 TOKEN_RING_10 TR   UP    UP    10-00-f1-0b-09-5f 06.02
  6 TOKEN_RING_7  TR   UP    UP    10-00-f1-0b-58-00 08.02

8260A>
```

Figure 117. Status Display for DMM Interfaces

This information allows you to determine which segments can be monitored by a T-MAC or E-MAC. In this example, we have two E-MACs assigned to Ethernet_1 and Ethernet_3 and two T-MACs assigned to token-ring_10 and token_ring_7 segments. Also, we have defined a SLIP interface for the DMM, but at the time of this display, the SLIP interface was not active. Note that the MAC addresses shown are those of the T-MAC and E-MACs, and the ″admin stat″ is as configured by ″SET MODULE INTERFACE″ command for the T-MAC or E-MAC. The ″admin stat″ should be ″UP″ for the DMM to be able to use that interface to monitor the corresponding network.

As shown in Figure 117, each E-MAC or T-MAC has an ″interface index″ assigned to it automatically. You must use this ″interface index″ in referring to the E-MAC and T-MAC in various monitoring commands as discussed later in this section.

The following sections provide a summary of monitoring functions provided by E-MAC and T-MAC.

Note

Readers are advised not to confuse the DMM ″MONITOR″ command with what we have called in this book the ″Monitoring Functions of DMM″.

10.6.1 Monitoring Functions Supported by E-MAC

E-MAC provides the following functions:

- Support for standard RMON MIBs:
  - RFC 1271 media independent

DMM (and E-MAC) allow you to collect the following RMON information for the Ethernet segments in your 8260:

- Host
- History
- Alarm
- Event
- Matrix
- Statistics
- TopN-hosts

10.6.2 Monitoring Functions Supported by T-MAC

T-MAC V2.0 provides the following functions:

- Support for standard RMON MIBs:
  - RFC 1271 media independent
    - Host group
  - RFC 1513 token-ring specific
    - MAC Layer Statistics group
    - Promiscuous Statistics group
    - Ring Station group
    - Ring Station Order
    - Ring Station Configuration group
    - Source Routing group
- Support for token-ring surrogate functions (IBM MIB extensions):
  - Configuration Report Server (CRS)
    - Ring station information
    - Removes station from ring
    - Reports topology changes
  - Ring Error Monitor (REM)
    - Monitors/collects/analyses errors
    - Assists in fault isolation
- DOT_5 group support
  - Support for RFC 1231 IEEE 802.5 Token-Ring MIB
- Support for MIB-II interface statistics

The following sections describe how you can monitor the token-ring and Ethernet segments on the 8260 using the monitoring capabilities offered by the T-MAC and E-MAC daughter cards.

Note: The following sections describe how you can collect and monitor the statistics VIA the DMM command interface ONLY. The other method is via SNMP using a client application which is not described in this book.

Note

The statistics that are collected using the DMM commands described in the next sections are NOT all RMON statistics. The non-RMON statistics are identified.

10.6.3 SHOW COUNTER Command for Ethernet Networks

This DMM command allows you to display the following information for the segments to which the DMM has an interface via an E-MAC:

1. Display error statistics for an Ethernet segment

   You can display the error statistics for Ethernet segments using the following command:

   `SHOW COUNTER ETHERNET {ethernet_n | isolated}`

   Note: These counters are not related to RMON.

   An example of the output displayed for this command is shown in Figure 118.

```
8260A> show counter ethernet ethernet_1


Ethernet Statistics for ETHERNET_1
------------------------------------------------------------------------------
FCS Errors                      0
SQE Test Errors                 0
Alignment Errors                0
Carrier Sense Errors            0
Frame Too Longs                 0
Deferred Transmissions           0
Late Collisions                 0
Excessive Collisions            0
Single Collision Frames         0
Multiple Collision Frames       0
Internal MAC Receive Errors     0
Internal MAC Transmit Errors    0


8260A>
```

Figure 118. Show Counter Ethernet

2. Display network statistics for an Ethernet segment

   You can display the network statistics for Ethernet segments using the following command:

   `SHOW COUNTER INTERFACE {ethernet_n | isolated}`

   Note: These counters are not related to RMON.

   An example of the output displayed for this command is shown in Figure 118.

```
8260A>
8260A> show counter interface ethernet_1


Interface Statistics for ETHERNET_1
-------------------------------------------------------------------------------
Received Octets                 939978
Received Unicast Packets        8488
Received Non-Unicast Packets    992
Received Discards               0
Received Errors                 0
Received Unknown Protocols      0
Transmitted Octets              256
Transmitted Unicast Packets     0
Transmitted Non-Unicast Packets 4
Transmitted Discards            0
Transmitted Errors              0


8260A>
```

Figure 119. Show Counter Interface for Ethernet Segment

3. Display statistics about the traffic from an individual port/module

   You can display the network statistics for an individual port or module using the following command:

   `SHOW COUNTER REPEATER {network} MODULE {slot} or`

   `SHOW COUNTER REPEATER {network} PORT {slot.port}`

   Note: These counters are not related to RMON.

   An example of the output displayed for this command is shown in Figure 120 on page 217.

```
8260A>
8260A> show counter repeater ethernet_1 module 2


Repeater Statistics for Module 2 on ETHERNET_1
------------------------------------------------------------------------------
Readable Frames                 0
Readable Octets                 0
Runts                           0
FCS Errors                      0
Late Events                     0
Short Events                    0
Frame Too Longs                 0
Very Long Events                0
Alignment Errors                0
Collisions                      0
Data Rate Mismatches            0
Auto Partition Count            0


8260A>
```

Figure 120. Show Counter Repeater for Ethernet Segment

Note: With the current release of the DMM code, we could not display this information about the 8250 Ethernet modules, regardless of where the E-MAC was installed.

4. Display RMON host statistics

   You can display the RMON Host group for stations attached to a segment using the following command:

   `SHOW COUNTER RMON HOSTS {network} {all | mac_address}`

   An example of the output displayed for this command is shown in Figure 121 on page 218.

```
8260A>
8260A> show counter rmon hosts ethernet_1 all


RMON Hosts Table for Host Address 00-00-c9-01-01-0b on Port 2.4
--------------------------------------------------------------------------------
Received Packets                136
Received Octets                 8704
Transmitted Packets             190
Transmitted Octets              13132
Transmitted Errors              0
Transmitted Broadcast Packets   0
Transmitted Multicast Packets   54




RMON Hosts Table for Host Address 80-00-7a-00-00-a0 on Port 0.0
--------------------------------------------------------------------------------
Received Packets                222
Received Octets                 19376
Transmitted Packets             0
Transmitted Octets              0
Transmitted Errors              0
Transmitted Broadcast Packets   0
Transmitted Multicast Packets   0


-- More --



8260A>
```

Figure 121. Show Counter RMON Hosts

In order to be able to collect the above statistics, you must have enabled RMON Host group collection using the following command:

```
SET RMON HOST INTERFACE {index}
```

Where *index* is the index number associated with the E-MAC attached to the network to be monitored. This index number can be displayed using the "SHOW INTERFACE" command.

Note: If the E-MAC is mounted on EC-DMM, you will be able to collect the above statistics about stations attached to both 8260 and 8250 modules. However, if the E-MAC is installed on an 8260 media module the statistics will only be collected for stations attached to the 8260 modules.

10.6.4 Collecting and Displaying RMON Groups Using E-MAC

DMM (and E-MAC) allow you to collect the following RMON groups for the Ethernet segments in your 8260:

- Host
- History
- Alarm
- Event
- Matrix

- Statistics
- TopN-hosts

To be able to collect and view the above information, you must perform the following steps:

1. Use the ″SHOW INTERFACE″ command to determine the *interface index* for each E-MAC installed in your hub.
2. Enable the E-MAC interface if not enabled already. You can do this using the following command for the E-MAC:

   ```
   set module {slot.subslot} interface enable
   ```

3. Enable the RMON probe function of the E-MAC using the following command:

   ```
   set module {slot.subslot} rmon_probe enable
   ```

   Note: Enabling the probe-mode function causes E-MAC to rest.

   Enabling the rmon_probe function on the E-MAC allows you to add and delete control table entries (as discussed in the next step) for the following RMON groups:

   - Statistics
   - Host
   - Matrix
   - History
   - Host Top N
   - Events
   - Alarms

4. To be able to collect the information about each RMON group, you must add the DMM interface to the RMON control table of that group. You can do this for each RMON group using the following commands:

   - Host group

     ```
     SET RMON HOST INTERFACE {interface index}
     ```

   - History group

     ```
     SET RMON HISTORY INTERFACE {interface index}
     ```

   - Statistics group

     ```
     SET RMON STATISTICS ETHERNET INTERFACE {interface index}
     ```

   - Matrix group

     ```
     SET RMON MATRIX INTERFACE {interface index}
     ```

   - Event group

     ```
     SET RMON EVENT {event_type} {interface index}
     ```

     The event_type can be as follows:

     – log
     – log_trap
     – trap
     – none

   - Alarm group

```
SET RMON ALARM ETHERNET {stat_type}.{interface} RISING {threshold}
         FALLING {threshold} {event} {time} {trigger} {alarm type}
```

The following is a summary of the parameters that can be specified for the Stat_type:

- BroadcastPackets
- Collisions
- CRCAlignErrors
- Fragments
- Jabbers
- MulticastPackets
- Octets
- OversizePackets
- Packets
- UndersizePackets

In the above command, *event* is the index number of the RMON event that occurs when the threshold is exceeded.

Note: You must issue the above commands for each DMM interface and for each RMON group that DMM is to collect statistics for. For example, to enable our DMM to collect RMON Host group for Ethernet_1, we added interface 3 to the RMON Host control table using the following command:

```
8260> set rmon host ethernet interface 3
```

Note

When you enable the probe-function of the DMM, it creates default control entries for:

- Collecting statistics on the MAC interface
- Monitoring host information
- Monitoring matrix information
- Generating two history reports, one every 30 seconds and one every 30 minutes.

- Verify that the appropriate entries in the RMON control tables have been created. You may do this by displaying the contents of the RMON control tables using the following command:

  ```
  SHOW RMON {rmon_group} CONTROL ALL
  ```

  In the above command, the rmon_group can be:

  - Alarm
  - Event
  - History
  - Host
  - Matrix
  - TopN_hosts

The format of the command to display the contents of the control table for the statistics group is slightly different. In this case, you must use the following command:

```
SHOW RMON statistics ETHERNET CONTROL ALL
```

The following example allows you to determine all the interfaces on which the RMON host group is enabled.

```
8260A> show rmon host control all

RMON Host Control Information:

Index Data Source     Table Size  Last Delete Time    Owner
----- --------------- ----------- ------------------- ----------------
    1 Interface 3              10 No Deletions        system


8260A>
```

Figure 122. RMON Host Control Table

As can be seen, at the time of display, the host group is only enabled on interface 3.

- Once the DMM interface is added to the appropriate RMON control table, the RMON information for that group will be collected on the network to which this interface is attached. You can display the contents of the RMON information for the desired group using the following command:

  ```
  SHOW RMON {rmon group} DATA {control_index} {data_index}
  ```

  In the above command, the control_index is the index for the RMON group that you want to display the information for. You can determine the control_index by displaying the RMON control table as shown in Figure 122. The data_index is the index of the specific collected information that you want to view. For more information about the values for data_index for various groups, please refer to the *DMM Command Guide,* SA33-0275.

  An example of how to display the RMON Host group output is shown in Figure 123 on page 222.

```
8260A> show rmon host data 1 all by_creation_order

RMON Host display for Interface 3 :

Creation Order                  : 1
Host Address                    : 10-00-5A-D4-B0-8C
Input Packets                   : 2954
Output Packets                  : 2954
Input Octets                    : 301308
Output Octets                   : 301308
Output Errors                   : 0
Output Packets (Broadcast)      : 0
Output Packets (Multicast)      : 0


Creation Order                  : 2
Host Address                    : 10-00-5A-82-5A-6A
Input Packets                   : 2963
Output Packets                  : 2963
Input Octets                    : 301960
Output Octets                   : 301960
Output Errors                   : 0
Output Packets (Broadcast)      : 0
Output Packets (Multicast)      : 0

-- More --

 ................

End of Host Table
```

Figure 123. RMON Host Statistics Display

10.6.5 SHOW COUNTER Command for Token-Ring Networks

This command allows you to display the following information about the segments to which the DMM has an interface via a T-MAC:

1. Display error statistics for a token-ring segment

   You can display the error statistics (DOT5) for token-ring segments using the following command:

   `SHOW COUNTER TOKEN_RING {token_ring_n}`

   Note: These counters are not related to RMON.

   An example of the output displayed for this command is shown in Figure 124 on page 223.

```
8260A>
8260A> show counter token_ring token_ring_7
Token Ring Statistics for TOKEN_RING_7
------------------------------------------------------------------------------
Ring Status:      No Problems Detected    Ring State:       Opened
Ring Open Status: Ring Open               Ring Speed:       4 MBPS
Upstream Station: 40-00-00-03-33-38       Functional Addr.: c0-00-00-00-00-18
Active Monitor Selection Participation:   Disabled


Line Errors:                    1
Burst Errors:                   7
AC Errors:                      0
Abort Transmitted Errors:       0
Internal Errors:                0
Lost Frame Errors:              0
Receiver Congestion Errors:     0
Frame Copied Errors:            0
Token Errors:                   2
Soft Errors:                    3
Hard Errors:                    0
Signal Losses:                  0
Transmit Beacons:               0
Recoveries:                     0
Lobe Wires:                     0
Removes:                        0
Singles:                        3

8260A>


8260A>
```

Figure 124. Show Counter for Token_Ring Segments

In the above example, the top portion of the display will always show the correct information regardless of the settings of the monitoring parameters for the T-MAC. But, to get the correct counter values (shown in the bottom part of the display), you must enable DOT5 Group for the T-MAC using the following command:

```
SET MODULE {slot.subalot} DOT5_GROUP enable
```

2. Display network statistics for a token-ring segment

   You can display the network statistics for token-ring (DOT5) segments using the following command:

   ```
   SHOW COUNTER INTERFACE {token-ring_n | isolated}
   ```

   Note: These counters are not related to RMON.

   An example of the output displayed for this command is shown in Figure 125 on page 224.

```
8260A> show counter interface token_ring_7


Interface Statistics for TOKEN_RING_7
------------------------------------------------------------------------------
Received Octets                 6082132
Received Unicast Packets        19226
Received Non-Unicast Packets    93810
Received Discards               0
Received Errors                 1
Received Unknown Protocols      0
Transmitted Octets              322275
Transmitted Unicast Packets     64
Transmitted Non-Unicast Packets 0
Transmitted Discards            0
Transmitted Errors              0


8260A>
```

Figure 125. Show Counter Interface for Token-Ring Segment

3. Display RMON host statistics

   You can display the RMON host statistics for stations attached to a token-ring segment using the following command:

   `SHOW COUNTER RMON HOSTS {network} {all | mac_address}`

   An example of the output displayed for this command is shown in Figure 126 on page 225.

```
8260A> show counter rmon hosts token_ring_7 all


RMON Hosts Table for Host Address 40-00-00-03-33-38 on Port 6.9
--------------------------------------------------------------------------------
Received Packets                0
Received Octets                 0
Transmitted Packets             203
Transmitted Octets              11108
Transmitted Errors              1
Transmitted Broadcast Packets   202
Transmitted Multicast Packets   1




RMON Hosts Table for Host Address 10-00-f1-0b-58-00 on Unk
--------------------------------------------------------------------------------
Received Packets                1
Received Octets                 26
Transmitted Packets             1
Transmitted Octets              26
Transmitted Errors              0
Transmitted Broadcast Packets   0
Transmitted Multicast Packets   0

-- More --

8260A>
```

Figure 126. Show Counter RMON Hosts for Token_Ring Segments

Note that in the above display, 10-00-f1-0b-58-00 is the MAC address of the T-MAC.

In order to be able to collect the above statistics, you must have enabled RMON host statistics collection using the following command for T-MAC:

`SET MODULE {slot.subslot} RMON_HOST_STATS enable`

4. Display RMON Ring_Station statistics

   You can display the RMON ring-station statistics for stations attached to a token-ring segment using the following command:

   `SHOW COUNTER RMON RING_STATION {network} {all | mac_address |ring}`

   An example of the output displayed when the ″ring″ option is used is shown in Figure 127 on page 226.

```
8260A> show counter rmon ring_station token_ring_7 ring

RMON Token Ring Station Control Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
Active Stations:        2
Table Size:             2
Ring State:             Normal operation
Last Beacon Sender:     00-00-00-00-00-00
Last Beacon NAUN:       00-00-00-00-00-00
Active Monitor:         40-00-00-03-33-38
Order Changes:          2

8260A>
```

Figure 127. Show Counter RMON Ring_station Using "ring" Option

An example of the output from the above command with the “all” option is shown in Figure 128 on page 227.

```
8260A>
8260A> show counter rmon ring_station token_ring_7 all
RMON Token Ring Station Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
Station Mac Address: 40-00-00-03-33-38  Station Status: Active
Last Enter Time:     1483081            Last Exit Time: 0
Last NAUN:           10-00-f1-0b-58-00
--------------------------------------------------------------------------------
Duplicate Addresses:    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:           1
In Beacon Errors:       0
Out Beacon Errors:      0
Insertions:             1


RMON Token Ring Station Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
Station Mac Address: 10-00-f1-0b-58-00  Station Status: Active
Last Enter Time:     1483083            Last Exit Time: 0
Last NAUN:           40-00-00-03-33-38
--------------------------------------------------------------------------------
Duplicate Addresses:    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:             1

8260A>
```

Figure 128. Show Counter RMON Ring_station Using "all" Option

In order to be able to collect the above statistics, you must have enabled RMON ring_station collection using the following command for T-MAC:

```
SET MODULE {slot.subslot} RMON_RING_STATION_STATS enable
```

5. Display RMON TR-MAC-LAYER statistics

   You can display the RMON tr_mac_layer statistics for stations attached to a token-ring segment using the following command:

SHOW COUNTER RMON TR_MAC_LAYER {network}

An example of the output displayed for this command is shown in Figure 129.

```
8260A>
8260A> show counter rmon tr_mac_layer token_ring_7
RMON Token Ring Mac-Layer Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
Drop Events:         0
Beacon Events:       0
Beacon Time:         0
Beacon Packets:      0
Claim Token Events:  0
Claim Token Packets: 0
MAC Octets:          432
MAC Packets:         12
NAUN Changes:        0
Ring Poll Events:    6
Ring Purge Events:   0
Ring Purge Packets:  0
Soft Error Reports:  0


Abort Errors:        0
AC Errors:           0
Burst Errors:        0
Line Errors:         0
Internal Errors:     0
Congestion Errors:   0
Frame Copied Errors: 0
Frequency Errors:    0
Lost Frame Errors:   0
Token Errors:        0

8260A>
```

Figure 129. Show Counter RMON TR_MAC_LAYER

In order to be able to collect the above statistics, you must have enabled RMON mac_layer_stats collection using the following command for T-MAC:

SET MODULE {slot.subslot} RMON_MAC_LAYER_STATS enable

6. Display RMON TR_PROMISCUOUS statistics

   You can display the RMON tr_promiscuous statistics for stations attached to a token-ring segment using the following command:

   SHOW COUNTER RMON TR_PROMISCUOUS {network}

   An example of the output displayed for this command is shown in Figure 130 on page 229.

```
8260A>
8260A> show counter rmon tr_promiscuous token_ring_7
RMON Token Ring Promiscuous Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
Data Octets:          27092
Data Packets:         472
DATA PACKETS
DATA PACKETSckets:    23
Broadcast Packets:    472
Multicast Packets:    02
18   to 63    Octets: 457
64   to 127   Octets: 15
128  to 255   Octets: 0
256  to 511   Octets: 0
512  to 1023  Octets: 0
1024 to 2047  Octets: 0
2048 to 4095  Octets: 0
4096 to 8191  Octets: 0
8192 to 18000 Octets: 0
> 18000       Octets: 0
8260A>
8260A>
```

Figure 130. Show Counter RMON TR_MAC_LAYER

In order to be able to collect the above statistics, you must have enabled RMON promiscuous_stats collection using the following command for T-MAC:

```
SET MODULE {slot.subslot} PROMISCUOUS_STATS enable
```

7. Display RMON TR_SOURCE_ROUTING statistics

   You can display the RMON tr_source_routing statistics for stations attached to a token-ring segment using the following command:

   ```
   SHOW COUNTER RMON TR_SOURCE_ROURING {network}
   ```

   An example of the output displayed for this command is shown in Figure 131 on page 230.

```
8260A> show counter rmon tr_source_routing token_ring_7
RMON Token Ring Source Routing Statistics for Network TOKEN_RING_7
--------------------------------------------------------------------------------
In      Frames:       0
Out     Frames:       0
Through Frames:       1013
In      Octets:       0
Out     Octets:       0
Through Octets:       93748
All    Rt Brcst Frms: 7477
Single Rt Brcst Frms: 18488
All    Rt Brcst Octs: 553319
Single Rt Brcst Octs: 2624628
Local LLC Frames:     559
One   Hop  Frames:    0
Two   Hops Frames:    0
Three Hops Frames:    0
Four  Hops Frames:    0
Five  Hops Frames:    0
Six   Hops Frames:    0
> Six Hops Frames:    0

8260A>
```

Figure 131. Show Counter RMON TR_SOURCE_ROUTING

In order to be able to collect the above statistics, you must have enabled RMON sr-routing_stats collection using the following command for T-MAC:

```
SET MODULE {slot.subslot} SR_ROUTING_STATS enable
```

10.6.6 Collecting and Displaying RMON Groups Using T-MAC

DMM (and T-MAC) allow you to collect information about the following RMON groups for token-ring segments:

- Host group
- MAC Layer Statistics group
- Promiscuous Statistics group
- Ring Station group
- Ring Station Order
- Ring Station Configuration group
- Ring Station Configuration group
- Source Routing group

To be able to collect and view the above information, you must perform the following steps:

1. Use the ″SHOW INTERFACE″ command to determine the *interface index* for each T-MAC installed in your hub. Note the ″interface index″ assigned to each T-MAC as you will use this ″index″ in the following command.
2. Enable the T-MAC interface if not enabled already. You can do this using the following command for the T-MAC:

   ```
   SET MODULE {slot.subslot} INTERFACE enable
   ```

3. Enable the collection of RMON information by T-MAC, using the following command:

   ```
   SET MODULE {slot.subslot} RMON_GROUP enable
   ```

   This command enables the collection of RMON information by T-MAC. You must, also, enable the collection of individual RMON groups using the commands described in the next step.

4. Use the following commands to enable the collection of information for individual RMON groups by T-MAC:

   - Host group

     ```
     SET MODULE {slot.subslot} RMON_HOST_STATS enable
     ```

   - MAC Layer Statistics group

     ```
     SET MODULE {slot.subslot} RMON_MAC_LAYER_STATS enable
     ```

   - Promiscuous Statistics group

     ```
     SET MODULE {slot.subslot} RMON_PROMISCUOUS_STATS enable
     ```

   - Ring Station Statistics group

     ```
     SET MODULE {slot.subslot} RMON_RING_STATION_STATS enable
     ```

   - Source Routing Statistics group

     ```
     SET MODULE {slot.subslot} RMON_SRC_ROUTING_STATS enable
     ```

   For example, to enable our DMM to collect RMON Host group statistics for token_ring_7, we used the following command:

   ```
   8260> set module 8.2 rmon_host_stats enable
   ```

5. Verify that the T-MAC is enabled to collect the appropriate RMON group, using the following example:

```
8260A>
8260A> show module 8.2 verbose

Slot  Module          Version Network       General Information
----- --------------- ------- ------------- -------------------
08.02 T-MAC           v2.00   TOKEN_RING_7

T-MAC: Token Ring Network Monitor Card

Boot Version:                             v2.00
IP Address:                               9.67.46.195
Subnetwork Mask:                          ff.ff.ff.f0
Default Gateway:                          0.0.0.0
Station Address:                          10-00-f1-0b-58-00
Locally Administered Address:             00-00-00-00-00-00
MAC Address Type:                         BURNED-IN
Interface Mode:                           ENABLED
RMON Groups:                              ENABLED
Surrogate Groups:                         DISABLED
Dot5 Group:                               DISABLED
RMON Host Statistics Collection:          ENABLED
RMON MAC Layer Statistics Collection:     ENABLED
RMON Promiscuous Statistics Collection: ENABLED
RMON Ring Station Statistics Collection: ENABLED


RMON Source Routing Statistics Collection: ENABLED
Monitor Contention:                       DISABLED
Adapter Status:                           OPENED
Adapter Microcode Version:                00 00 01 c1 e3 f1 f7 c3 f1 40
Early Token Release:                      DISABLED
Internal Wrap:                            DISABLED
External Wrap:                            DISABLED
Interface Number:                         6


8260A>
```

Figure 132. Show Module Command for T-MAC

As can be seen, at the time of display, all the RMON groups are enabled on the T-MAC.

6. Once the T-MAC is enabled to collect the appropriate RMON group, you can display the collected information using the following command:

   `SHOW COUNTER RMON {rmon group} {network}`

   This command is described in 10.6.5, “SHOW COUNTER Command for Token-Ring Networks” on page 222.

10.7 Surrogate Functions Supported by T-MAC

The token-ring architecture defines the Configuration Report Server (CRS) and Ring Error Monitor (REM) functions.

The Ring Error Monitor (REM) observes, collects, and analyzes hard-errors and soft-error reports sent by the ring stations on a single ring and assists in fault isolation and correction. Configuration Report Server (CRS) function accepts commands from the LAN manager to get station information, set station

parameters, and remove stations on its ring. It also collects and forwards configuration reports generated by stations on its ring to the LAN manager.

Traditionally, CRS and REM functions are implemented in the bridges. However, the 8260 T-MAC implements the CRS and REM functions, which provides you with the following functions:

- Collect soft error statistics
- Analyze soft error statistics
- Collect Beaconing statistics
- Analyze Beacon frames
- Report Beacon conditions and resolutions
- Report REM MAC frames
- Provide ring station configuration information
- Report NAUN and Active Monitor changes
- Forced removal of stations off the ring

10.7.1 Using T-MAC Surrogate Functions

To be able to use the T-MAC surrogate functions, you must do the following:

1. Enable the surrogate features
2. Enable the individual surrogate groups

10.7.1.1 Enabling Surrogate Features

Enabling the surrogate feature on the T-MAC results in the Ring Error Monitor (REM) and Configuration Report Server (CRS) functions of the T-MAC to be activated. To enable the surrogate features you must do the following:

1. Enable the surrogate function

   You can use either of the following commands to enable the surrogate function:

   ```
   SET MODULE {slot.subslot} SURROGATE_GROUP enable or

   SET TR_SURROGATE {slot.subslot} SURR_STATUS SURR_ADMIN enable
   ```

   Note: Surrogate function must be enabled before you can enable the CRS or REM function.

2. Enable the REM feature using the following command:

   ```
   SET TR_SURROGATE {slot.subslot} SURR_STATUS REM_ADMIN
   ```

3. Enable the CRS feature using the following command:

   ```
   SET TR_SURROGATE {slot.subslot} SURR_STATUS CRS_ADMIN
   ```

4. Enable the Surrogate Ring feature using the following command:

   ```
   SET TR_SURROGATE {slot.subslot} SURR_STATUS RING_SEGMENT
   ```

You may display the status of the surrogate features using the following command:

```
SHOW TR_SURROGATE {slot.subslot} SURR_STATUS
```

An example of the output from this command is shown in Figure 133 on page 234.

```
8260A> show tr_surrogate 8.2 surr_status

Surrogate Status Data for Network TOKEN_RING_7
------------------------------------------------------------------------
Surrogate Admin Status:         ENABLED
Port Mac Address:               10-00-f1-0b-58-00
Ring Segment:                   0000
Ring Utilization:               0.0%
REM Admin Status:               ENABLED
REM Oper Status:                Active
CRS Admin Status:               ENABLED
CRS Oper Status:                Active

8260A>
```

Figure 133. Displaying the Status of Surrogate Features

10.7.1.2 Enabling Individual Options within the Surrogate Groups

Once the surrogate features are enabled, you may enable the individual surrogate options within the surrogate groups, using the following commands:

```
SET TR_SURROGATE {slot.subslot} REM_STATUS {options}

SET TR_SURROGATE {slot.subslot} CRS_STATUS {options}

SET TR_SURROGATE {slot.subslot} CRS_STATIONS {options}
```

For details of the permitted options, please refer to the *DMM Command Guide*, SA33-0275.

You can display the status of individual options within each surrogate group using the following commands:

- Status of REM options

  ```
  SHOW TR_SURROGATE {slot.subslot} REM_STATUS
  ```

  An example of the output from this command is shown in Figure 134 on page 235.

```
8260A> show tr_surrogate 8.2 rem_status

Ring Error Monitor Status Data for Network TOKEN_RING_7
--------------------------------------------------------------------------------
REM Traps:                        DISABLED
Weight Exceeded Traps:            DISABLED
PreWeight Exceeded Traps:         DISABLED
Receiver Congestion Traps:        DISABLED
NonIso Threshold Exceeded Traps: DISABLED
Forward Frames Traps:             DISABLED
Ring Line Error Data:             DISABLED
Ring Internal Error Data:         DISABLED
Ring Burst Error Data:            DISABLED
Ring AC Error Data:               DISABLED
Ring Abort Xmitted Error Data:    DISABLED
Ring Lost Frames Error Data:      DISABLED
Ring Receiver Congestion Data:    DISABLED
Ring Frame Copied Data:           DISABLED
Ring Frequency Error Data:        DISABLED
Ring Token Error Data:            DISABLED


Auto Line Error Data:             DISABLED
Auto Internal Error Data:         DISABLED
Auto Burst Error Data:            DISABLED
Auto AC Error Data:               DISABLED
Auto Abort Xmitted Error Data:    DISABLED
Auto Lost Frames Error Data:      DISABLED
Auto Receiver Congestion Data:    DISABLED
Auto Frame Copied Data:           DISABLED
Auto Frequency Error Data:        DISABLED
Auto Token Error Data:            DISABLED
Ring State:                       Normal
Reset:                            Reset Complete

8260A>
```

Figure 134. Displaying the Status of REM Options

- Status of CRS options

  SHOW TR_SURROGATE {slot.subslot} CRS_STATUS

  An example of the output from this command is shown in Figure 135.

```
8260A> show tr_surrogate 8.2 crs_status

Configuration Report Server Status Data for Network TOKEN_RING_7
--------------------------------------------------------------------------------
CRS Traps:               DISABLED
NAUN Changes:            0
Active Monitor Changes:  0
Tx Forward Strip Status: 0000

8260A>
```

Figure 135. Displaying the Status of CRS Options

- Status of CRS Stations options

  SHOW TR_SURROGATE {slot.subslot} CRS_STATION ALL

An example of the output from this command is shown in Figure 136 on page 236.

```
8260A> show tr_surrogate 8.2 crs_station all

Configuration Report Server Ring Station Data for MAC address 10-00-f1-0b-58-00
of Network TOKEN_RING_7
------------------------------------------------------------------------------
Station Status:         Active
Mfg. Adapter Address:   10-00-f1-0b-58-00
NAUN Address:           40-00-00-03-33-38
Functional Address:     00-00-00-18
Group Address:          ff-ff-ff-ff
Microcode Level:        000001c1e3f1f7c3f140
Microcode Status:       100000904e00
Product Id:             20202020202020202020202020202020
Function Class Mask:    7b7f
Max. Token Priority:    0003
Physical Location:      00000000



Configuration Report Server Ring Station Data for MAC address 40-00-00-03-33-38
of Network TOKEN_RING_7
------------------------------------------------------------------------------
Station Status:         Active
Mfg. Adapter Address:   10-00-5a-89-c5-dc
NAUN Address:           10-00-f1-0b-58-00
Functional Address:     00-00-00-01
Group Address:          00-00-00-00
Microcode Level:        000000c3f2f4f5f5f040
Microcode Status:       000011700200
Product Id:             0110f0f0f0f0f0f0f0f0f0f0f0f0f0f0f0
Function Class Mask:    7b7f
Max. Token Priority:    0003
Physical Location:      00000000

8260A>
```

Figure 136. Displaying the Status of CRS Stations Options

10.7.2 Displaying the Information Collected by Surrogate Features

Once the surrogate features and groups are enabled, you can use the following commands to display the collected information:

- REM error MAC frames

  SHOW TR_SURROGATE {slot.subslot} REM_ERROR_MAC_FRAME

- REM isolating errors

  SHOW TR_SURROGATE {slot.subslot} REM_ISOLATING

- Last Beacon received by REM

  SHOW TR_SURROGATE {slot.subslot} REM_LAST_BEACON

- Last soft error received by REM

  SHOW TR_SURROGATE {slot.subslot} REM_LAST_SOFT_ERROR

- Non-isolating soft error

```
SHOW TR_SURROGATE {slot.subslot} REM_SOFT_ERROR
```

- Threshold exceeded conditions

```
SHOW TR_SURROGATE {slot.subslot} REM_THRESHOLD_EXCD
```

10.8 DOT5_Group Support by T-MAC

DOT5_Group support by T-MAC allows you to perform the statistics collection tasks defined in the IEEE 802.5 token-ring Management Information Base (MIB). These functions allow the T-MAC to perform the following:

- Collect soft error statistics
- Provide interface status information

10.8.1 Using DOT5_Group Functions

To enable the T-MAC to collect token-ring statistics (dot5), you must use the following command:

```
SET MODULE {slot-subslot} DOT5_GROUP enable
```

The information collected by the DOT5 Group can be displayed using the following command:

```
SHOW COUNTER TOKEN_RING {token_ring_n}
```

10.9 Summary of T-MAC Monitoring Functions

The following table provides a summary of the monitoring functions supported by T-MAC 2.0.

Table 34. Functions Supported by T-MAC V2.0

Function	RMON	CRS	REM	DOT5
Collects information and forwards the information upon request	X	X	X	X
Analyzes information collected			X	
Assists in fault isolation			X	
Reports unsolicited error conditions			X	
Reports unsolicited ring topology changes		X		
Provides information to DMM for more dynamic address-to-port mapping	X			

The following table indicates more details on what data each T-MAC function uses.

Table 35 (Page 1 of 2). Functions Performed by T-MAC V2.0

Function	RMON	CRS	REM	DOT5
Provides Soft Error statistics	X		X	X
Analyzes Soft Error statistics			X	
Provides Beaconing statistics	X		X	
Analyzes Beacon frames			X	

Table 35 (Page 2 of 2). Functions Performed by T-MAC V2.0

Function	RMON	CRS	REM	DOT5
Reports Beaconing conditions & resolution			X	
Reports REM MAC frames			X	
Provides ring station configuration information	X	X		
Reports NAUN and Active Monitor changes		X		
Upon request, forces station off ring	X	X		
Provides local ring traffic stats	X			
Provides local ring stations stats	X			
Provides bridged/remote station stats	X			
Provides source routing statistics	X			
Provides interface state info				X

The definitions for the terminology used within the above table are:

- Analyzes = interprets the data that is collected
- Provides = sends solicited information on data collected
- Reports = sends unsolicited information on data collected

Chapter 11. 8260 Multiprotocol Interconnect Module

This chapter provides an overview of the routing and bridging functions provided by the Multiprotocol Interconnect module as well as discussing the steps required to configure the module to perform these functions.

In this document, we have assumed that the reader is familiar with routing and bridging protocols.

11.1 Introduction

The 8260 Multiprotocol Interconnect module is a one or two-slot module for the 8260 which allows you to interconnect Ethernet, 802.3, and token-ring networks using bridging and/or routing functions. These modules provide 6 ports for backplane attachments to the Ethernet segments on the ShuntBus or TriChannel. Additionally, the two-slot module provides you with the capability to install two additional I/O cards for providing connection to external token-ring and/or Ethernet networks. These additional I/O cards will provide the seventh and eighth port on the module. At the time of writing this book, the following I/O cards are available:

- Token-ring 4/16 I/O card
- Ethernet 10Base-T I/O card
- Ethernet 10Base-2 I/O card
- Ethernet 10Base-5 I/O card

Note that the I/O cards for the two-slot module only provide attachment capability to the external networks. For example, installation of the token-ring I/O card does not provide the ability to connect the module to the token-ring segments on the backplane.

The one-slot module can perform the following functions:

- Transparent bridging between Ethernet/802.3 segments
- IP routing between Ethernet/802.3 segments
- IPX routing between Ethernet/802.3 segments
- DECnet Phase IV routing between Ethernet/802.3 segments

The two-slot module can perform the following functions:

- Transparent bridging between Ethernet/802.3 segments
- Transparent bridging between token-ring segments operating at 4 and/or 16 Mbps
- Source route transparent bridging between token-ring segments operating at 4 and/or 16 Mbps
- Translational bridging between token-ring and Ethernet or 802.3 segments when both sides use transparent bridging
- IP routing between Ethernet/802.3 and/or token-ring segments
- IPX routing between Ethernet/802.3 and/or token-ring segments
- DECnet Phase IV routing between Ethernet/802.3 segments

Note: DECnet Phase IV routing is not supported on token-ring ports.

The Multiprotocol Interconnect module uses a 32-bit RISC processor (80960FA) for high performance, allowing you to forward up to 45,000 packets per second when bridging and up to 30,000 packets per second when routing IP. The performance of the module will vary depending on the number of routing protocols running in the module as well the size of the packets.

This module can be managed using a local ASCII terminal (VT100/VT220) connected to the module through an RS-232 port (locally or via a dialup modem operating at speeds up to 9600 bps). It can also be managed remotely using Telnet.

The Multiprotocol Interconnect module, also supports SNMP allowing it to be managed using an SNMP manager.

New software can be downloaded to the Multiprotocol Interconnect module using BOOTP, TFTP, or X-Modem. This can be done:

1. Out-of-band - Using a local or modem attached PC to the RS-232 port on the module.
2. Inband - Using an IP network

The management facilities of the Interconnect module allow you to:

- Configure the module for bridging and/or routing functions
- Monitor traffic counters
- Monitor diagnostics information
- Monitor address table information for routing and bridging functions

The Multiprotocol Interconnect module consists of:

1. Backplane Interface Module (BIM):

   This module provides the following functions:

   - Connection to the ShuntBus and Enhanced TriChannel Ethernet/802.3 segments
   - A DB-9 connector for local management
   - Housing for two additional I/O cards (2-slot module only)

2. Router Engine Module (REM):

   This module is installed on the BIM and provides housing for an i960 processor.

3. I/O cards (available on the two-slot module):

   Up to two I/O cards (in any combination) can be installed on the BIM to provide connections for up to two external token-ring and/or Ethernet segments.

Note

The connectors on the token-ring I/O modules are via DB-9 connectors.

Figure 137 on page 241 shows the front view of the 1-slot and 2-slot Multiprotocol Interconnect modules.

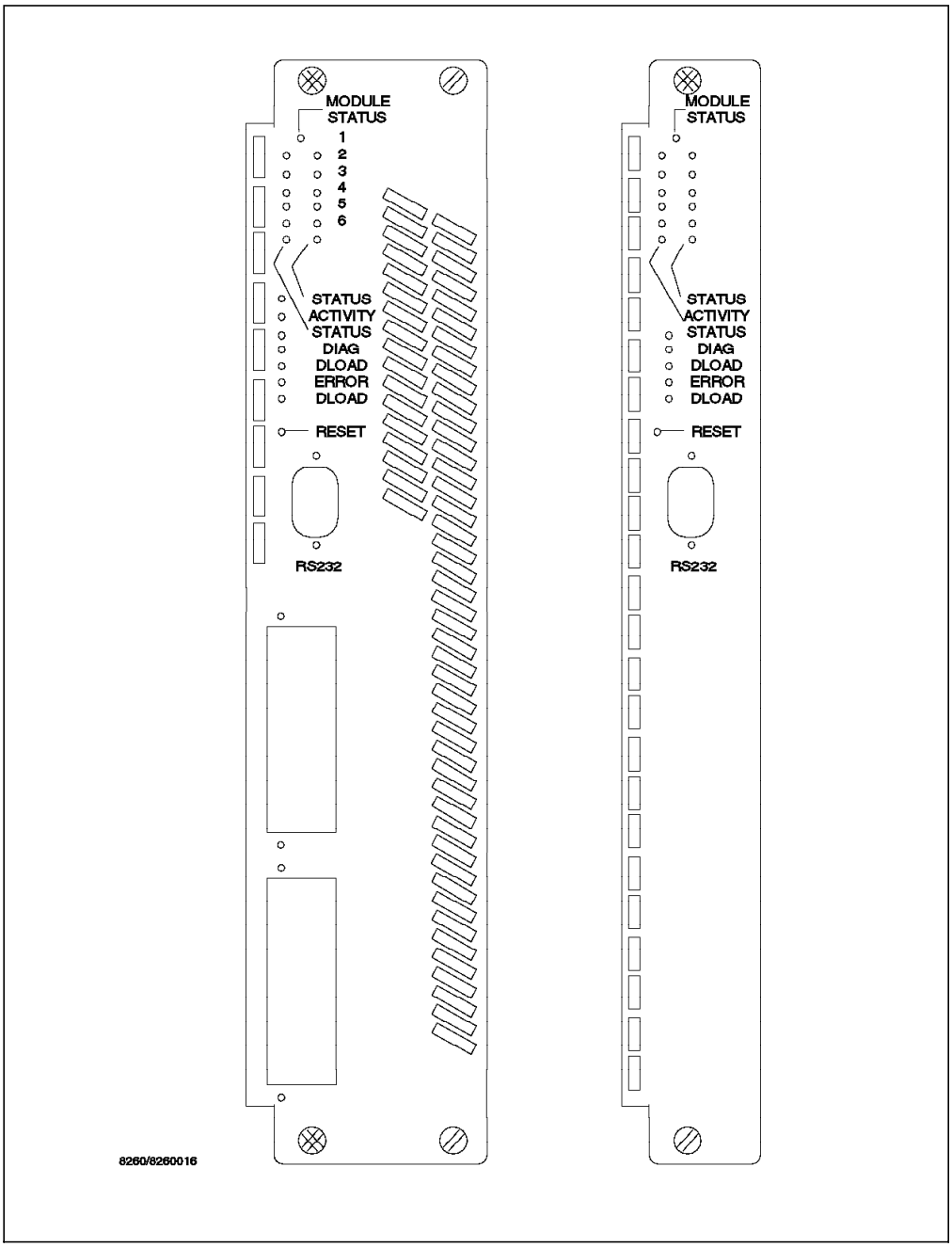


Figure 137. Front View of the Multiprotocol Interconnect Modules

There are a number of activity and status LED displays on the front panel of the Multiprotocol Interconnect module which are used to show the information provided in Table 36 on page 242.

Table 36. Interconnect Module LED Description

LED Name	Color	State	Description
Module Status	Green	On	Power is on, software functioning
		Off	Power is off or complete failure
		Blinking	Power is on but diagnostics failure
Network Activity	Yellow	On	Continuous activity on the port
		Off	No activity on this port
		Blinking	Normal activity on this port
Network Status	Green	On	Port assigned to a network
		Off	Port isolated
		Blinking	Fault detected on this network
Status	Green	On	Online
		Off	Fault
		Blinking	Normal operations
DIAG	Green	On	POST being run
		Off	Normal operation
		Blinking	Error detected
Error	Green	On	Error
		Off	Normal operation
		Blinking	Major error
DLOAD	Yellow	On	Download in progress
		Off	Normal operation
		Blinking	Error detected

11.2 Power Requirements for Multiprotocol Interconnect Module

Certain 8260 modules will not completely support the inventory management scheme that has been employed with the media modules and daughter cards. Typically every 8260 module board contains an inventory EEPROM, which the controller module reads to determine the total power requirements of a slot (motherboard plus any connected daughter cards). In the case of the Multiprotocol Interconnect module, the I/O cards that connect to the module do not support the inventory management scheme. This is because these I/O cards are not populated with EEPROMs as other 8260 daughter cards. There is only one EEPROM on the Multiprotocol Interconnect module itself to report the power requirements of the entire module. The issue that arises is that there is significant variation in the amount of power these I/O cards consume as shown in Table 37. This requires that the user must be able to update the power requirements of the Multiprotocol Interconnect module to reflect the current I/O card configuration and ensure proper and accurate operation of the inventory and power management system.

Table 37 (Page 1 of 2). Power Requirements for Interconnect Module IP Cards

I/O Cards	Total Power Requirements (in Units)				
	+2V	+5V	-5V	+12V	-12V
Interconnect Module	-	30	4	1	-

Table 37 (Page 2 of 2). Power Requirements for Interconnect Module IP Cards					
I/O Cards	**Total Power Requirements (in Units)**				
	+2V	**+5V**	**-5V**	**+12V**	**-12V**
10Base-5	-	9	-	8	-
10Base-2	-	8	-	3	-
10Base-T	-	7	-	-	-
Token-Ring	-	9	-	-	1

It is expected that the customer will buy the Multiprotocol Interconnect module pre-configured with I/O cards, including proper programming for EEPROM, and will leave the I/O card configuration, as is, for extended periods of time. It is when the user decides to alter the I/O configuration that the information in the EEPROM needs to be changed to reflect the power requirements of the new configuration. To change the programmed EEPROM I/O requirements, you must do the following:

1. Determine the total power requirements of the module using the information provided in Table 37 on page 242.
2. Establish that there is sufficient power in the hub using the following DMM command:

   ```
   SHOW POWER BUDGET
   ```

   Note that because the 8260 measures the amount of power required by each I/O card in units, you must convert the watts available for each voltage type to units, using the conversion factor for each voltage type as shown in Table 38.

Table 38. Watts to Units Conversion Table	
Voltage Type	**Watts to Units Conversion**
+5V	1 Watt = 1 Unit
-5V	.25 Watt = 1 Unit
+12V	.5 Watt = 1 Unit
-12V	.25 Watt = 1 Unit
+2V	.1 Watt = 1 Unit

3. Put DMM in Maintenance mode using the following DMM command:

   ```
   MAINTAIN
   ```

4. While in Maintenance mode, enter the following command:

   ```
   SET POWER MODULE {slot.subslot} POWER_REQUIREMENT
   ```

5. You will be prompted to enter the following:

   ```
   Enter +5V power requirements in units of 1 Watt:
   Enter -5V power requirements in units of .25 Watt:
   Enter +12V power requirements in units of .5 Watt:
   Enter -12V power requirements in units of .25 Watt:
   Enter +2V power requirements in units of .1 Watt:
   ```

   Note that you must enter the above prompts in units.

6. Enter the response to the above prompts using Table 37 on page 242.
7. You will be prompted with the following:

```
Do you want to enter this into module x.y's EEPROM (Y/N):
```

8. Enter *Y* in response to the above prompt.
9. Remove the module from the 8260 and install the I/O card.
10. Return DMM to normal operation using the following command:

    ```
    BOOT
    ```

11. Install the module in the 8260. Now the module will report accurate power requirements of the entire module.

11.3 Bridging Functions

This module can perform transparent bridging (TB) between Ethernet or 802.3 segments as well as between token-ring segments. Also, it can be configured to perform source-route transparent (SRT) bridging between token-ring networks. Finally, it can perform translational bridging between token-ring and Ethernet (or 802.3) networks when both the token-ring and Ethernet (or 802.3) segments are using transparent bridging.

Note

This module cannot perform source-route to transparent (SR-TB) bridging like the IBM 8209 and 8229.

This module supports the spanning tree protocol and can coexist and interoperate with other transparent and source-route transparent bridges that support the spanning tree protocol.

Note

This module cannot use the spanning tree protocol to interoperate with source route (SR) bridges.

When performing transparent bridging functions, it dynamically learns the addresses of all the nodes on the subnetworks. To do so, the module looks at the source address of each packet and creates a database containing these addresses. You can also configure the filtering database with permanent entries to build a customized bridging environment. When a packet is received by the module, its destination is compared with the addresses in the database entries for that subnetwork. If it is found, the station is considered to be local and the packet will not be forwarded. If the address is not found, the station is considered to be in a subnetwork other than the source subnetwork and the packet will be forwarded on some or all the ports depending on how you have configured your bridge. For information about filtering databases and the filtering options provided by the Multiprotocol Interconnect module, refer to 11.8.5, “Filtering for Bridging Functions” on page 270.

As a source-route transparent bridge, this module will use the routing information field (RIF) in the frame to forward the packet towards its destination.

This module can also be configured to bridge the traffic between token-ring and Ethernet (or 802.3) networks. In bridging traffic between token-ring and Ethernet (or 802.3) it also supports IPX traffic.

11.4 Routing Functions

The Multiprotocol Interconnect module supports the following routing protocols:

- IP
- IPX
- DECnet Phase IV

11.4.1 IP Routing Support

When acting as an IP router, the Multiprotocol Interconnect module provides support for:

- Directed broadcast
- ICMP
- Proxy ARP
- Ethernet or 802.3 (not both) encapsulation on LAN interface
- Datagram fragmentation/reassembly support
- IP security
- Boothelper
- Static routes
- Dynamic routes
  - RIP
  - OSPF

11.4.1.1 RIP Implementation

The following is a summary of the RIP implementation in the Multiprotocol Interconnect module:

- Routing messages are broadcast every 30 seconds.
- Triggered updates are sent.
- ″Split horizon with poison reverse″ is always used.
- Host level routing is supported (with future WAN I/O cards).
- RIP can be enabled/disabled on a per logical port basis.
- RIP can be enabled/disabled globally.
- Path cost can be configured on each logical port.
- Routing table entries are aged-out to ensure validity of routes.
- Can pass or block datagrams according to user defined security access list.

11.4.1.2 OSPF Implementation

The following is a summary of the OSPF implementation in the Multiprotocol Interconnect module:

- Only topology changes are broadcast as per OSPF Specification Version 2 (RFC 1247).
- Supports alternate routes based on IP Type Of Service (TOS).
- Supports multiple paths with equal costs.

- Supports authentication between routers.
- Importation of RIP routes and static routes to an OSPF domain may be enabled or disabled.
- Filters may be configured to import or discard specific RIP and static routes to OSPF.
- Supports hop count to OSPF metric conversion when importing RIP and static routes.
- Does not support non-broadcasting multi-access networks (such as X.25).

11.4.2 IPX Routing Support

The following is a summary of the IPX implementation in the Multiprotocol Interconnect module:

- Supports RIP (Routing Information Protocol) and SAP (Service Advertising Protocol).
- Supports split horizon.
- Does not support poison reverse.
- Does not support split path routing.
- Does not support static RIP or SAP entries.
- Does not support equal cost paths.
- Can pass or block datagrams according to user defined security access list.

11.4.3 DECnet Phase IV Routing Support

The Multiprotocol Interconnect module in a DECnet environment is always a level 2 router. It implements the DECnet routing layer and provides network management and security, including the following:

- Supports configurable circuit cost.
- Supports designated router priority.
- Supports designated router priority.
- Can pass or block datagrams according to user defined security access list.

DECnet routing is not addressed any further in this book.

11.5 Configuring Multiprotocol Interconnect Module

Both one-slot and two-slot Multiprotocol Interconnect modules provide six ports that can be attached to any of the Ethernet segments on the ShuntBus or Enhanced TriChannel. These ports are referred to as ports 1 thru 6. Additionally, the 2-slot module provides the housing for two I/O cards that can be used to provide connections to external token-ring and/or Ethernet segments. These ports are referred to as ports 7 and 8.

To configure the 8260 Multiprotocol Interconnect module, you must use the Local Management Systems (LMS) accessed via the local (or remote) console.

Once you have completed the configuration of a Multiprotocol Interconnect module using the facilities offered by LMS, you must use the following MM

command to assign ports 1 thru 6 to the desired Ethernet segments on the ShuntBus or Enhanced TriChannel.

```
SET PORT {slot.port} NETWORK {ethernet_n|isolated}
```

Note that ports 7 and 8 are not assigned to any segment on the backplane; therefore, the above command is not required for these ports.

11.6 Local Management System (LMS)

When you connect to the Interconnect module via an ASCII terminal or Telnet session, you can have one of the following two types of sessions:

1. Write session

   In this type of session you can alter configuration parameters and view statistics related to the Multiprotocol Interconnect module.

2. Read session

   In this type of session you can view the configuration parameters and statistics related to the Multiprotocol Interconnect module.

Up to a maximum of four users can access LMS. One of these can be through the local or modem connected console and the others will be via Telnet sessions. Only one user can have write access at a time, which allows that user to modify the configuration of the module.

Once you connect to the LMS, the initial menu of the LMS as shown in Figure 138 is displayed.

```
                              6706I-E            Module: BladeRunner
                                                 Time:   12:42  5 Jan 95


                          Configuration Menu

                          Status Menu

                          Enable Write Access

                          Help

                          Close Connection









                      Enter the Config Environment
```

Figure 138. LMS Initial Panel

The following is a brief description of each selectable option on the initial LMS menu:

- *Configuration Menu*

  This option allows you to alter configuration parameters and monitor statistics about the Multiprotocol Interconnect module.

- *Status Menu*

  This option allows you to review the statistics and configuration information without changing any values.

- *Enable/Disable Write Access*

  When you first access the LMS, you automatically have read-only access to monitor the Multiprotocol Interconnect module. Write permission is protected by a password. If you want to modify configuration parameters, you must select *Enable Write Access* from the menu and enter the correct password. Alternatively, you may press CTRL-W from any menu to toggle write permission *On* or *Off* (an * will appear on the left of the screen title when you have write permission).

  The Multiprotocol Interconnect module is shipped from the factory with no password. This can be changed by using *Change Password* from the *System Parameters Screen* as discussed in 11.8.1, “Configuring System Wide Parameters” on page 252.

  Note: There can be only one user with write access at any one time. Therefore, if another user has accessed the Multiprotocol Interconnect module and has enabled write access, you will be unable to enable write access. There can be a total of four users accessing the LMS simultaneously.

- *Help*

  This option provides you with the list of shortcut commands which you can use to navigate through the LMS screens. The short cut commands are shown in Figure 139 on page 249.

```
       *                  Help Screen              Module: BladeRunner
                                                   Time:   13:07  5 Jan 95

control-C:          Cancel input, cancel a popup menu, or exit a screen

control-J:          Go to the screen jump table

control-K:          Go to this help screen

control-L:          Refresh the screen display

control-P,
control-T:          Go to the top of the menu hierarchy

control-W:          Toggle write access for this session

control-X:          Jump to the equivalent screen in the other mode



                                    Exit

                         Return to the previous screen
```

Figure 139. LMS Short Cut Commands

Most of the commands displayed in Figure 139 are self-explanatory but the following paragraphs deal with a couple of the commands which may require explanation.

Jump table provides you with a shortcut facility to view the screen you desire without having to traverse through the menu tree. To use the Jump table, you need to know the name of the screen you want to view. Figure 140 on page 250 shows the contents of the Jump table.

To use the Jump table, move the cursor to highlight the name of the screen you want to view then press Enter. The selected screen is then displayed.

When using CTRL-W to toggle from read-only to write access, you will be prompted to enter the write password. Also, if someone else is running a write session with this module, this command will not be available.

```
Config *          Jump Table - Config screens     Module: BladeRunner
                                                  Time:   14:25  5 Jan 95

System              Download            Trap Dest. Table    Physical Port List
Phy. Port Protocol  Phy. Port Interface Logical Port        Logical Port MLink
Bridging System     Bridging Port       STP System          STP Port
Filtering Database  Custom Filter Test  Custom Filter Stmt. Src. Routing System
Conversion System   IP System           IP Port             IP Port Address
IP NetToMedia Table IP Forwarding       IP Security List    IP Security Table
IP BootHelper       IP Ping             DECnet System       DECnet Port
DECnet Area Routing DECnet Routing      DECnet Sec. List    DECnet Sec. Table
IPX System          IPX Port            IPX Routing         IPX SAP Bindery
IPX Security List   IPX Security Table  OSPF System         OSPF Area Table
OSPF Area Def. Met. OSPF Address Range  OSPF Host           OSPF Interface
OSPF IF Metric      OSPF Virtual IF     OSPF Neighbor       OSPF RIP Filter
OSPF RIP Convert    OSPF RIP Def. Conv. OSPF Static Filter  OSPF Static Convert
OSPF St. Def. Conv.



                     Status Screens              Exit

                       Return to the previous screen
```

Figure 140. LMS Jump Table

- *Close Connection*:

  This option will only be displayed if you have accessed the Multiprotocol Interconnect module using Telnet. In that case, this option allows you to close the connection when required.

11.7 SNMP Support

The Multiprotocol Interconnect module provides an SNMP agent which can be used to manage the Multiprotocol Interconnect module via an SNMP manager. To access the SNMP agent, the SNMP manager is required to provide the correct *community name* as defined in the Multiprotocol Interconnect module. The process of defining community names for the Multiprotocol Interconnect module is described in 11.8.1, “Configuring System Wide Parameters” on page 252.

Depending on the community name settings, the SNMP agent may support any of the following options for an SNMP manager:

- Get-request
- Get-next-request
- Set-request
- Get-response
- Trap

The following MIBs are supported by the SNMP agent:

- MIB-II
- Dot1dBridge Group

- Dot5 Group
- Frame Relay Group
- IP Forward Group
- OSPF Group
- PPPF Group
- Retix Private MIB extensions

The following SNMP traps will be sent by the SNMP agent to the SNMP managers which have been defined as a *trap receiver*.

- coldStart
- linkUp
- Enterprise specific traps:
  - frDCLiStatusChange
  - newRoot
- Retix Enterprise specific traps:
  - logicalPortUp
  - logicalPortDown
  - fpUp
  - fpDown
  - hardwareFail
  - temperatureOverheat
  - powerSupplyFail

11.8 Configuring the Interconnect Module Using LMS

To configure the Multiprotocol Interconnect module, you must have a *write* session and must select *configuration* from the initial LMS menu. The panel shown in Figure 141 on page 252 will be displayed.

Using this panel you can configure the following features:

- System wide parameters
- Port parameters
- Bridging parameters
- Routing parameters

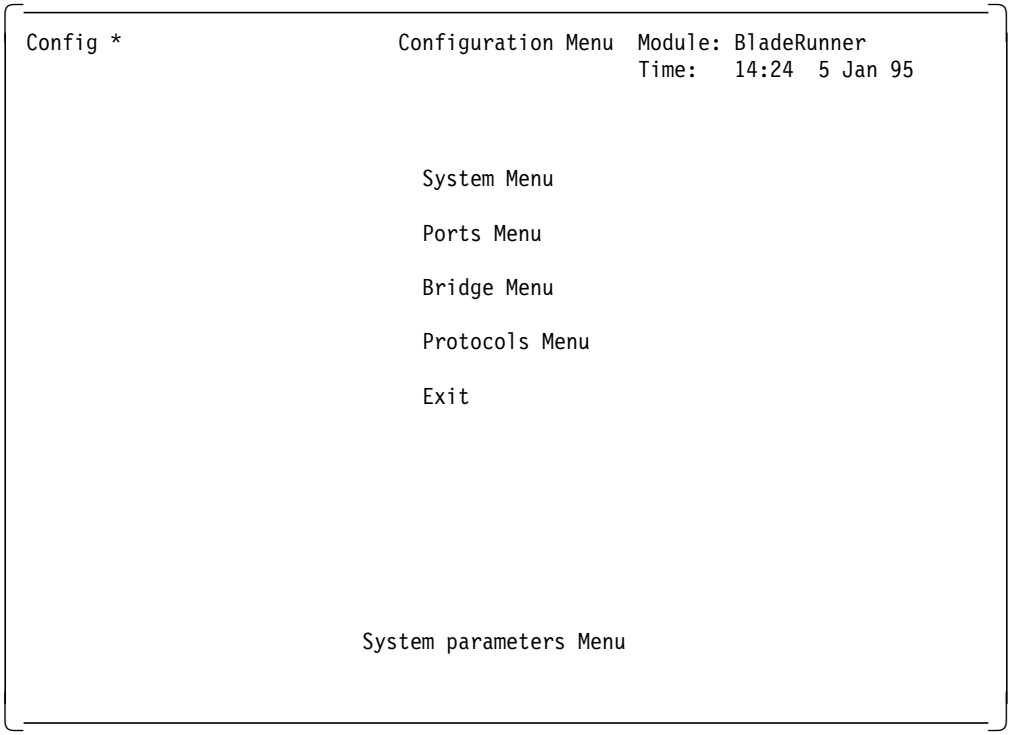


Figure 141. LMS Configuration Panel

The following sections will describe the required steps for configuring these features.

11.8.1 Configuring System Wide Parameters

The system wide parameters allow you to configure the following:

1. System Parameters

   This panel will allow you to configure the following:

   - *Name*

     Up to 64 characters used to uniquely identify the Multiprotocol Interconnect module.

   - *Location*

     Up to 64 characters used to identify the location of the Multiprotocol Interconnect module.

   - *Contact*

     Up to 64 characters used to identify the person responsible for the Multiprotocol Interconnect module.

   - *Station Time*

     Allows you to set the *date* and *time* for the Interconnect module.

   - *Next Reset*

     Allows you to determine the action to be taken on the next *Reset* of the module. The following can be specified:

     – *Coldstart*: All the configuration settings are set to the factory default.

– *Warmstart*: All the configuration settings are read from the FLASH memory, resulting in the restoration of the last *saved* configuration information. Note that all the statistics tables will be cleared during to a *Warmstart*.

The *Menu Bar* options of the *Systems Parameters* screen allow you to perform the following:

- *Reset Unit*

  This enables you to initiate an immediate reset of the Interconnect module. When you choose this option, you will be prompted to enter *Reset* or *Cancel* to proceed.

- *Change Password*

  This allows you to change the module's password for *write access*. The length of the password can be up to 64 characters and you will be prompted to enter the password twice.

- *Exit*

  Allows you to return to the previous (Configuration Menu) screen.

An example of the System Parameters panel is shown in Figure 142.

```
Config *                System Parameters           Module: BladeRunner
System                                              Time:   14:29  5 Jan 95

Name:          BladeRunner

Location:      ITSO Lab, Raleigh

Contact:       Mohammad Shabani X2339

Station Time: 14:29  5 Jan 95

Next Reset:    warmStart









            Reset Module        Change Password          Exit

                        Return to the previous screen
```

Figure 142. LMS System Parameters Panel

2. Trap Destination Table

   As shown in Figure 143 on page 254, this panel allows you to specify the SNMP managers to which the *Traps* are sent.

   There can be up to a maximum of eight entries specified in this table and each entry contains the following parameters identifying an SNMP manager and its authority:

   - *IP Address*
   - *Community Name*

To add an entry to this table, you must select *Add Entry* from the *Menu Bar* options of the panel shown in Figure 143 on page 254. You will then be prompted (via a pop-up menu) to enter the IP address and the community name of the SNMP manager. After entering this information you must select (on the pop-up menu) *Set Entry* to add this entry to the table or *Cancel* to abandon the operation.

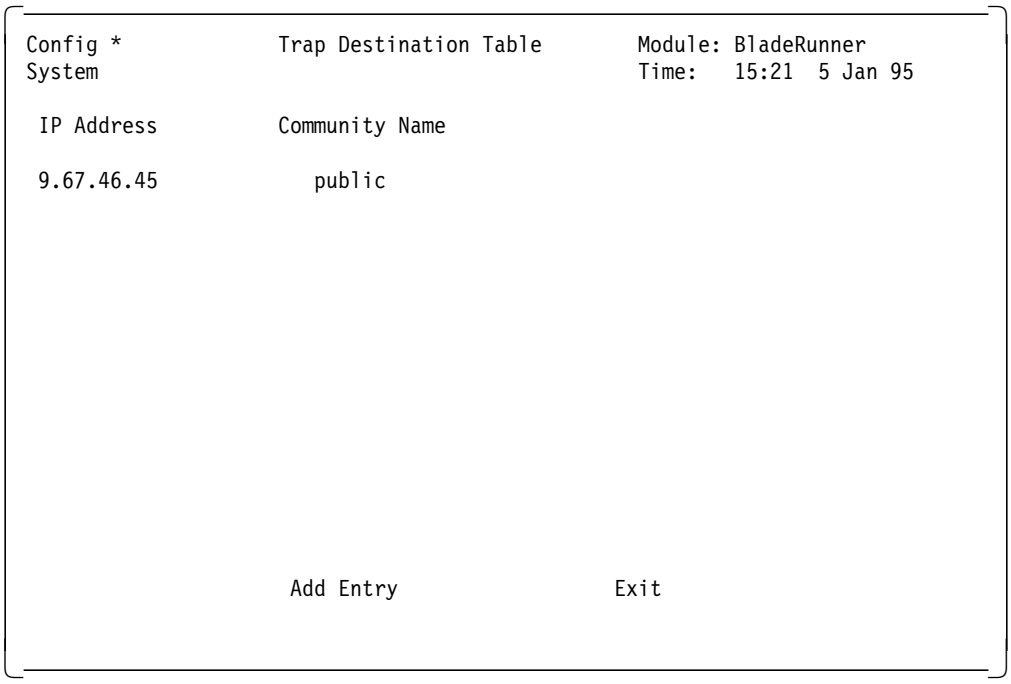


Figure 143. LMS Trap Destination Panel

3. Download Parameters

   You can download new software into the Multiprotocol Interconnect module using one of the following two ways:

   - Using BOOTP/TFTP over the network
   - Using a PC attached to the Multiprotocol Interconnect module's RS-232 port

   Download Parameters panel shown in Figure 144 on page 255 allows you to specify the download method to be used and also allows you to start the operation.

   Using this panel, you must enter the following parameters for the BOOTP/TFTP method:

   - *TFTP Server IP Address*
   - *TFTP Filename*

   Once the above parameters are entered, you can select *Start BOOTP Download* to start the download. The *TFTP Status* field on the screen will display the current status of the TFTP operation.

Note

If you select *Start BOOTP Download* and do not specify the TFTP server IP address and TFTP filename in the above panel, the Multiprotocol Interconnect module will use BOOTP to locate a BOOTP server in the network in order to get this information to perform the download operation.

To perform download from a PC attached to the Multiprotocol Interconnect module's serial port, select *Start Serial Download*.

```
Config *              Download Parameters          Module: BladeRunner
System                                             Time:   15:26  5 Jan 95

TFTP Server:    9.67.46.45              TFTP Status: idle

TFTP Filename:  bld.op

   Start Serial Download            Start BootP Download            Exit
```

Figure 144. LMS Download Parameters Panel

11.8.2 Configuring Port Parameters

To configure the ports on the Multiprotocol Interconnect module, you must select *Port Menu* from the *Configuration Menu*. The panel shown in Figure 145 on page 256 will be displayed.

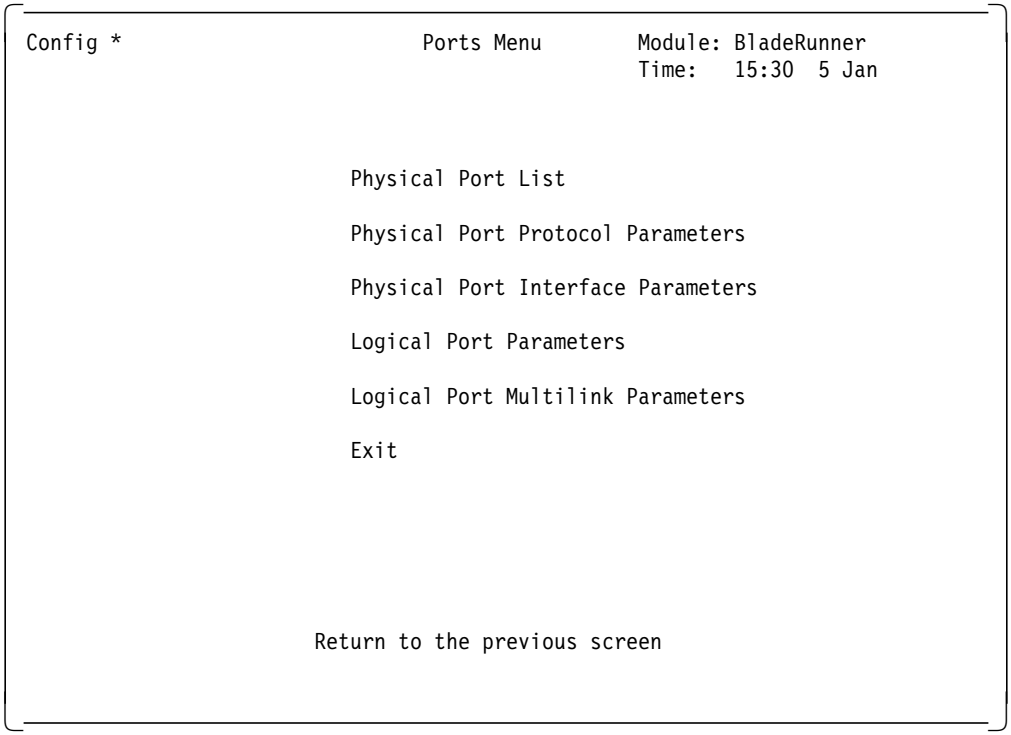


Figure 145. LMS Port Menu Panel

The parameters shown in this panel are each applicable to certain environments as described below:

- *Physical Port List*

  This option is applicable to all the WAN and LAN ports. Note that at the time of writing this book, IBM was not offering any I/O card for WAN connection.

- *Physical Port Protocol Parameters*

  This option is applicable to WAN and token-ring ports. It does not apply to Ethernet ports.

- *Physical Port Interface Parameters*

  This option is applicable to WAN ports only; therefore, we will not cover it in the remainder of this book.

- *Logical Port Parameters*

  This option allows you to configure logical ports for the Multiprotocol Interconnect module. LAN logical ports are created automatically (one per physical port) and take the number of the physical port on which they reside. When using a Multiprotocol Interconnect module with LAN only attachments, you do not need to perform any action using this panel.

  WAN logical ports can be created by entering a port number in the range (13-253) and attaching it to a WAN physical port. As WAN I/O cards are not currently available for the Multiprotocol Interconnect module, this process will not be discussed in this book.

- *Logical Port Multilink Parameters*

  This option allows you to provide load sharing over a number of WAN logical ports to the same destination. Therefore, Logical Multilink Ports are not

applicable to the LAN ports and will not be discussed any further in this book.

11.8.2.1 Configuring Physical Port Parameters

The *Physical Port List* panel displays information about the physical ports currently installed on your module. An example of this panel is shown in Figure 146.

```
Config *              Physical Port List            Module: BladeRunner
System                          Page 1              Time:   15:39  5 Jan 95

Port ID    Name              Connection    Card   Type        Protocol

  1        PHYSICAL PORT     Ethernet-1    0      Backplane   csmaLan

  2        PHYSICAL PORT     Isolated      0      Backplane   csmaLan

  3        PHYSICAL PORT     Isolated      0      Backplane   csmaLan

  4        PHYSICAL PORT     Isolated      3      Backplane   csmaLan

  5        PHYSICAL PORT     Isolated      3      Backplane   csmaLan

  6        PHYSICAL PORT     Isolated      3      Backplane   csmaLan



              Prev Page            Next Page            Exit

                       Return to the previous screen
```

Figure 146. LMS Physical Port List for Ethernet Connections

Note that the above panel also shows the list of backplane Ethernet connections for ports 1 thru 6. As can be seen from this panel, port 1 was assigned to Ethernet_1 segment on the backplane using DMM commands.

Selecting the *Next Page* option on this panel allows you to display the port list for any I/O cards that may be installed on your Multiprotocol Interconnect module. In our example, we had two token-ring I/O cards, so the resulting display is shown in Figure 147 on page 258.

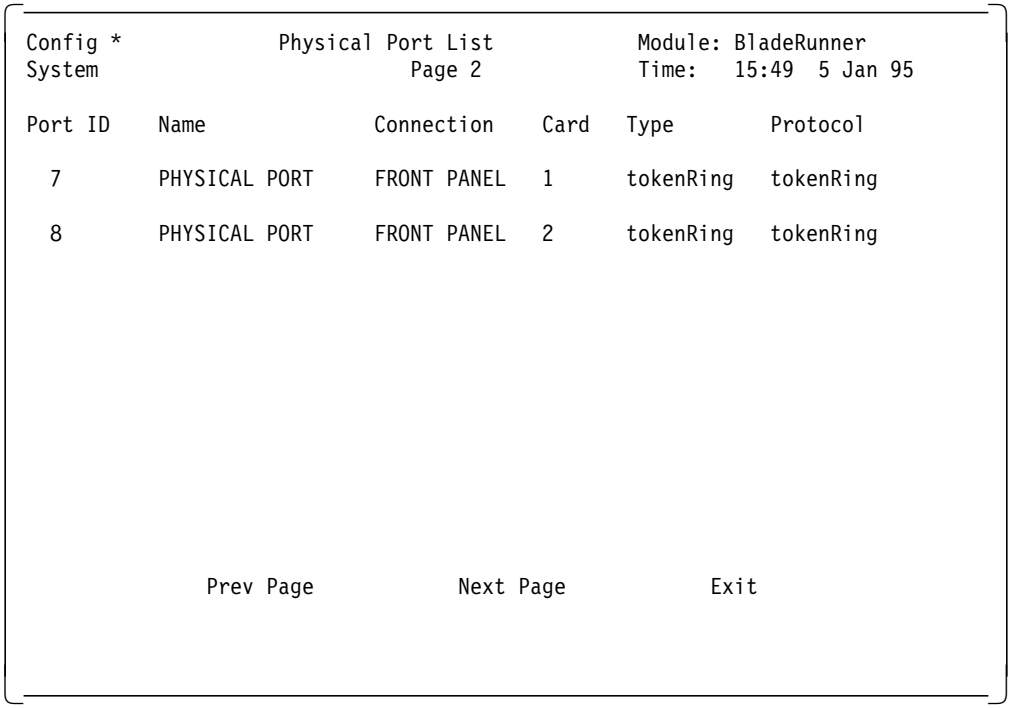


Figure 147. LMS Physical Ports List for Token-Ring I/O Cards

Using the *Physical Port List* panel, you may configure a *name* for each LAN port.

To configure a particular entry, select the entry and press the Enter key. A pop-up menu as shown in Figure 148 on page 259 will be displayed which allows you:

- To configure a name for the physical port.
- To configure a new protocol for the port. This option is only available for the WAN ports.
- To change the configuration of the protocol on the port. This option is only available for the token-ring and WAN ports. It is not applicable to Ethernet ports.

  Note: This pop-up menu is the same as that displayed when selecting *Physical Port Protocol Parameters* from the *Port Menu*.

11.8.2.2 Configuring Physical Port Protocol Parameters

An example of the *Physical Port Protocol Parameters* panel for a token-ring I/O card is shown in Figure 148 on page 259.

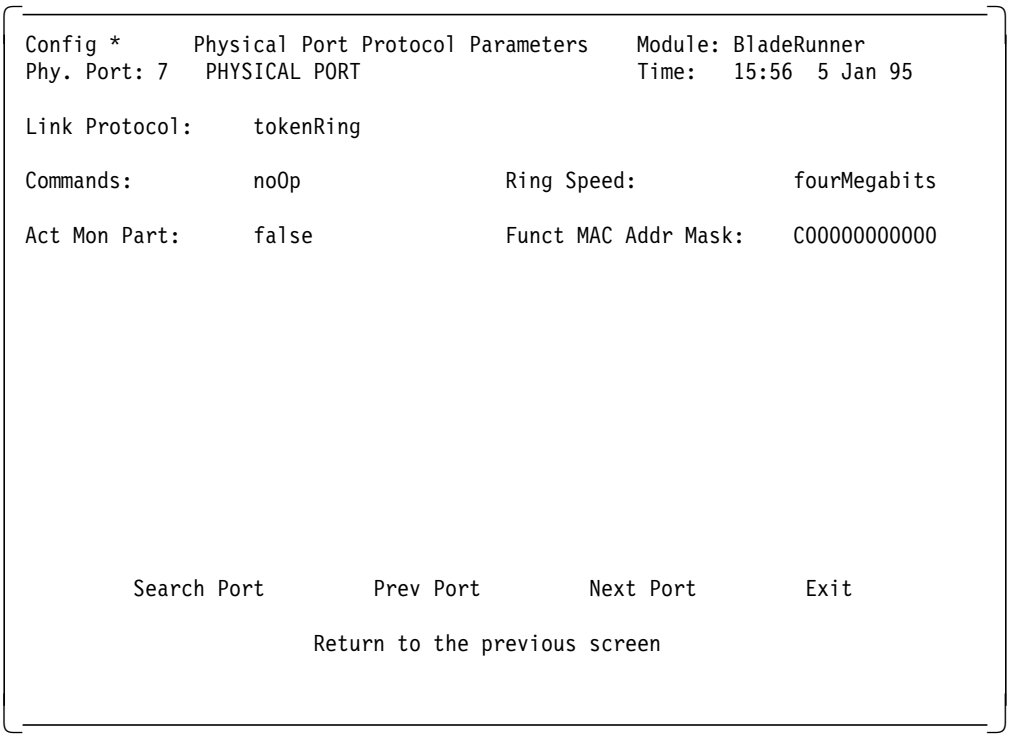


Figure 148. LMS Physical Port Protocol Configuration Panel

This panel allows you to specify the following options:

- *Commands*

  This entry allows you to configure the operational status of the token-ring port. The following options are available:

  - Open: tells the adapter to enter the ring.
  - Close: tells the adapter to remove itself from the ring.
  - Reset: causes an immediate reset of the token-ring port.
  - Noop: has no effect; it simply indicates that an open operation has not been requested.

- *Ring Speed*

  This parameter allows you the set the speed at which the token-ring port will operate.

- *Act Mon Par*

  This parameter allows you to specify if the station is to participate in the active monitor selection process. The choices for this parameter are:

  - True
  - False

- *Funct MAC Addr Mask*

  This parameter allows you to specify the bit mask that is applied to all functional addresses for which this port accepts frames.

11.8.2.3 Configuring Logical Port Parameters

This panel allows you to configure parameters for Ethernet, token-ring and WAN logical ports. An example of this panel for an Ethernet port is shown in Figure 149.

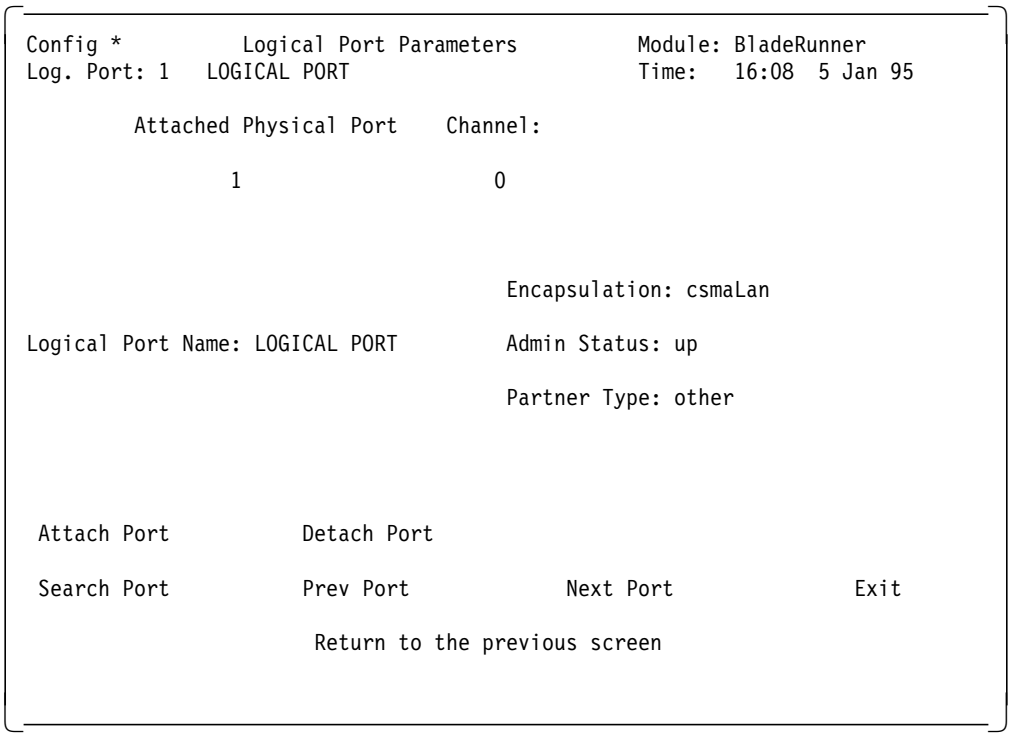


Figure 149. LMS Logical Port Panel

This panel allows you to enter/display the following parameters:

- *Attached Physical Port*

  This is a read-only parameter and identifies the physical port to which this entry applies.

  In the case of LAN logical ports, they will be created automatically and will be attached to a physical port with the same port ID. For example, logical port 1 will be attached to physical port 1, etc.

- *Channel*

  This parameter does not apply to LAN ports.

- *Logical Port Name*

  This parameter can be used to configure a unique name for the selected logical port.

- *Admin Status*

  This parameter shows the desired status of the logical port. *Up* means that the port is configured and can receive or transmit frames. When the status is *Down*, the port is configured but cannot send or receive frames.

- *Partner Type*

  This parameter specifies the type of partner that this logical port is connected to. On LAN ports, this parameter is set to *other* and cannot be changed.

- *Encapsulation*

  This is a read-only parameter and shows the type of encapsulation used on the physical port to which this logical port is attached. In the case of a token-ring port, this field will show *tokenRing*.

- *Attach Port* and *Detach Port*

  These parameters are used to attach/detach logical ports to/from WAN physical ports. They are not applicable to LAN ports.

11.8.3 Port Configuration Summary

The following is the summary of the steps you may need to perform for each port on the Multiprotocol Interconnect module:

1. Using *Physical Port List* panel assign a *name* to each LAN port.
2. For token-ring ports only, use the *Physical Port Protocol Parameter* panel to specify the following:
   - Ring speed for the adapter
   - Functional addresses for which this adapter accepts frames
   - Whether or not the adapter should contend to become an active monitor
3. Using the *Logical Port Parameters* panel assign a name to each logical port.

11.8.4 Configuring for Bridging Support

To configure the Multiprotocol Interconnect module for bridging, you must select the *Bridge Menu* from the *Configuration Menu*. This panel allows you to display and modify the configuration parameters relevant to the bridging function(s) of the Multiprotocol Interconnect module. The bridge menu panel is shown in Figure 150.

```
Config *                          Bridge Menu       Module: BladeRunner
                                                    Time:   16:30  5 Jan 95



                        Bridging System Parameters
                        Transparent Bridging Port Parameters
                        Source Routing Port Parameters
                        STP System Parameters
                        STP Port Parameters
                        Filtering Database
                        Custom Filter Test Table
                        Custom Filter Statement Table
                        Conversion System Parameters
                        Exit









              Enter the Transparent Bridging System Parameters screen
```

Figure 150. LMS Bridge Menu Panel

The following sections describe the procedures used to configure the Multiprotocol Interconnect module to perform one of the following:

- Transparent bridging for Ethernet and/or token-ring
- Source-route transparent bridging for token-ring
- Translational bridging between token-ring and Ethernet

11.8.4.1 Configuring for Transparent Bridging

After configuring the system-wide and port parameters, you must do the following:

1. Select *Bridging System Parameters* from the *Bridge Menu*. A panel as shown in Figure 151 will be displayed.

```
Config *   Bridging System Parameters              Module: BladeRunner
System                                             Time:   16:38  5 Jan 95

Bridging Facility: Enabled              Adaptive Routing Support: Disabled

Time To Delete:  86400                  Time To Forget:           300

SRT Bridge Number: Disabled

                                        Exit

                          Return to the previous screen
```

Figure 151. LMS Bridging System Parameters

This panel allows you to display and modify the system-wide bridging parameters for the Multiprotocol Interconnect module. To be able to perform transparent bridging only, the following options must be specified:

- *Bridging Facility* must be *enabled*.

  Note that this parameter (which is enabled by default), enables the bridging at the module level. As we will see in the next step, you must additionally enable bridging at each port which is to perform transparent bridging.

  If the bridging facility is *disabled*, the packet forwarding/filtering and learning functions are not performed on any of the ports regardless of the setting of the bridging parameters on the ports.

- *SRT Bridge Number* must be set to *disabled* when performing transparent bridging only.

- You may, optionally, modify the following parameters:

– *Time-To-Delete* (in seconds)

For information on this parameter, refer to 11.8.5, “Filtering for Bridging Functions” on page 270.

– *Time-To-Forget* (in seconds)

For information on this parameter, refer to 11.8.5, “Filtering for Bridging Functions” on page 270.

- You must ignore the following parameter as it does not apply to LAN only Multiprotocol Interconnect module:
  – *Adaptive Routing Support*

2. Select *Transparent Bridging Port Parameters* from the *Bridge Menu*. A panel as shown in Figure 152 will be displayed.

```
Config *    Transparent Bridging Port Parameters   Module: BladeRunner
Log. Port: 1   LOGICAL PORT                        Time:   16:54  5 Jan 95

Bridging Facility:          Enabled

Security Mode:              Disabled     Custom Filtering:          Disabled

Source Address Learning:    Enabled      Source Address Filtering:  Disabled

Always Accepts Multicasts: Disabled      Tinygram Compression:      Disabled









        Search Port         Prev Port         Next Port         Exit

                      Return to the previous screen
```

Figure 152. Transparent Bridging Port Parameters Panel

This panel allows you to configure the transparent bridging parameters for each port. Note that the information on the screen applies to the port identified on the top left corner of the panel. You can select the desired port by using *Search Port*, *Prev Port* and *Next Port* options from the *Menu Bar*.

To be able to perform bridging on each port, you must enable the *Bridging Facility* for that port.

Optionally, you may modify the following parameters for each port, depending on the filtering and security requirements of your network.

- *Security Mode*

  If *enabled*, the module searches the filtering database for the destination address of each packet to be bridged. If the address is not fixed (manually entered by the user), the packet is discarded. If the address is fixed, the packet is forwarded on the appropriate port.

If security mode is *disabled*, and the destination address is known, the packet is forwarded on the appropriate port. If the address is not known, the packet is sent (flooded) on all the other ports. For more information, refer to 11.8.5, “Filtering for Bridging Functions” on page 270.

- *Custom Filtering*

  This option allows you to *enable* or *disable* custom filtering for the packets received on this port. When this parameter is enabled, the *Custom Filter Test and Custom Filter Statement Table* will specify the tests and actions to be performed. For more information refer to 11.8.5, “Filtering for Bridging Functions” on page 270.

- *Source Address Learning*

  If *enabled*, the Multiprotocol Interconnect module will search the filtering database for the source address of each received packet. If the address in not found to be in the database, it will be added to the database along with the number of the port on which the packet was received.

- *Source Address Filtering*

  If *enabled*, the Multiprotocol Interconnect module will search the filtering database for the source address of each received packet. If the address in not a fixed entry (manually entered by the user in the filtering database), then the packet is discarded. Note that when security mode and source address filtering are both enabled, the bridged traffic is restricted to between the stations that have fixed entries in the database.

- *Always Accept Multicast*

  This parameter is used to allow the bridging of multicast packets when the security mode is enabled. If this parameter is disabled and the security mode is enabled, the multicast packets will be discarded. This parameter has no significance when the security mode is disabled.

Note: *Transparent Bridging Port Parameters* panel for token-ring ports is identical to that of the Ethernet ports which is shown here.

3. Select the *STP System Parameters* from the *Bridge Menu*. A panel as shown in Figure 153 on page 265 will be displayed.

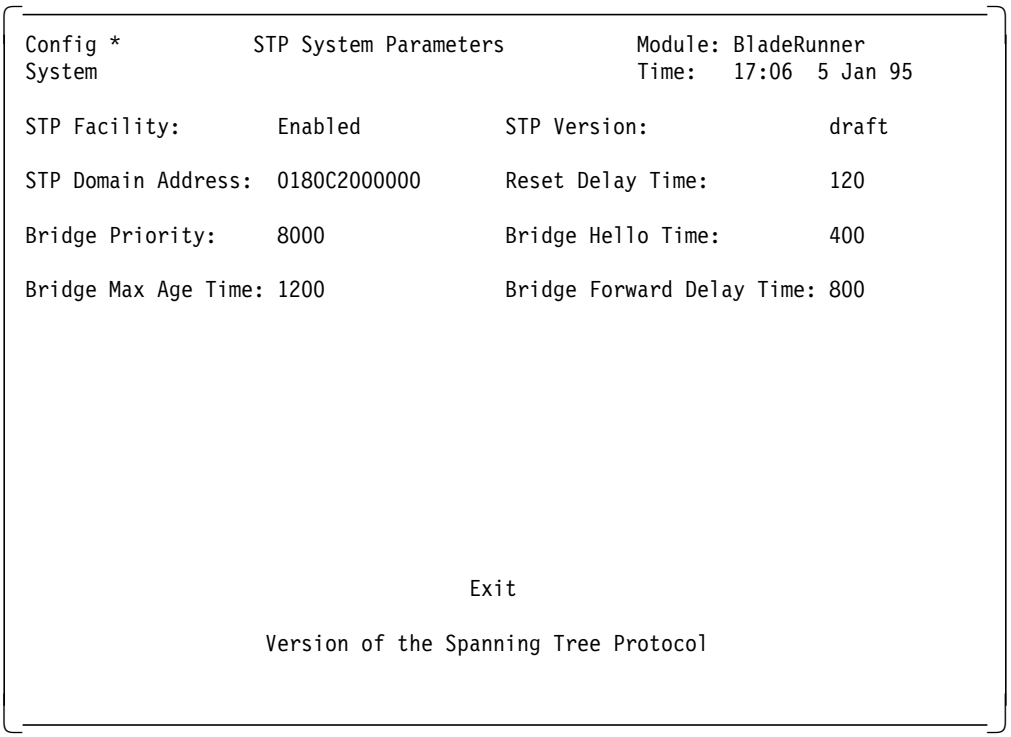


Figure 153. LMS STP System Parameters Panel

This panel allows you to view and modify the following system-wide spanning tree protocol (STP) parameters:

- *STP Facility*

  If *enabled*, this parameter allows the Multiprotocol Interconnect module to take part in the spanning tree protocol.

- *Bridge Hello Time*

  Specifies the frequency (in hundredths of a second) with which the Hello BPDUs will be transmitted by the Multiprotocol Interconnect module should this module become the *root* bridge.

- *STP Domain Address*

  This parameter specifies the address to which the Hello BPDUs will be sent. This parameter must be the same for all the bridges to have a single spanning tree within the network. Default for this entry is 0180C2000000.

- *Bridge Forward Delay Time*

  Specifies the length of time (in seconds) the bridge will remain in each of the intermediate states (*learning* and *listening*) when it is going from the *blocking* to *forwarding* state.

- *Bridge Priority*

  This parameter is used to determine the *root* bridge in the spanning tree. The bridge with the highest priority (lowest numeric value for bridge priority) becomes the root bridge. This is also used to determine the *designated* bridge when the path cost to the root bridge is the same for two or more bridges.

If two bridges have the same bridge priority, the one with the lowest MAC address has higher priority.

- *Bridge Max Age Time*

  Specifies the max value for the age field (in hundredths of a second) in the Hello BPDU before it is discarded by the Multiprotocol Interconnect module. This value will only be used (by all the bridges in the spanning tree as well as the Multiprotocol Interconnect module) should this module become the root bridge.

- *STP Version*

  This parameter specifies the version of the spanning tree protocol operating in the module. The options are *Revision_C* and *Draft_9*. Revision_C is a proprietary version of the protocol.

4. Select the *STP Port Parameters* from the *Bridge Menu*. A panel as shown in Figure 154 will be displayed.

```
Config *            STP Port Parameters            Module: BladeRunner
Log. Port: 1   LOGICAL PORT                        Time:   17:16  5 Jan 95

STP Facility: Enabled                   Manual Port Path Cost: 32768

Port Priority: 80                       Path Cost Mode: normal









        Search Port         Prev Port         Next Port         Exit

                      Return to the previous screen
```

Figure 154. LMS STP Port Parameters Panel

This panel allows you to specify the spanning tree parameters for the specified port. Note that the port number that these parameters apply to is displayed on the top left hand corner of the panel. You can use the *Search Port*, *Prev Port* and *Next Port* options from the menu bar to select the port for which you want to set these parameters. The parameters that can be specified are:

- *STP Facility*

  This parameter allows you to enable or disable the operation of the spanning tree on this port. To enable this parameter, the STP facility on the *STP System Parameters* panel must also be enabled.

  Note that when STP is disabled for a port, that port still learns addresses and forwards packets as normal.

- *Path Cost Mode*

  This parameter is used by the spanning tree protocol to determine how the value of the path cost is configured. The following values can be specified for this parameter:

  – *Manual*: In this case the path cost will be taken from the *Manual Port Path Cost* parameter.

  – *High*: The path cost will be determined by the 1000/LineSpeed formula.

  – *Normal*: The path cost will be determined by the 100/LineSpeed formula.

  – *Low*: The path cost will be determined by 10/LineSpeed formula.

  Note: *LineSpeed* is the speed of attached LAN in Mbps.

- *Manual Port Path Cost*

  This parameter specifies the path cost to be used when the *Path Cost Mode* is set to *manual*.

- *Port Priority*

  Used by the spanning tree protocol to determine which port will be the root port on the Multiprotocol Interconnect module when another port has the same path cost as the root port on the STP segment to which it is attached.

5. Optionally, you may set the security and filtering parameters as described in 11.8.5, “Filtering for Bridging Functions” on page 270.

11.8.4.2 Configuring for Source-Route Transparent Bridging

Configuring for source-route transparent bridging is similar to the configuration for transparent bridging with the following differences:

1. Configure the *Bridging Systems Parameters* as described in 11.8.4.1, “Configuring for Transparent Bridging” on page 262 with the following exception:

   - You must assign a *bridge number* in the range (0-15) to your Multiprotocol Interconnect module using the *SRT Bridge Number* parameter. When you assign a bridge number, you effectively enable the Multiprotocol Interconnect module as a source-route transparent bridge.

2. Configure transparent bridging parameters for the port(s) which are to perform source-route transparent bridging as described in 11.8.4.1, “Configuring for Transparent Bridging” on page 262. Note that the Multiprotocol Interconnect module is shipped with transparent bridging enabled for each port.

3. Select *Source Routing Port Parameters* from the *Bridge Menu*. A panel as shown in Figure 155 on page 268 will be displayed.

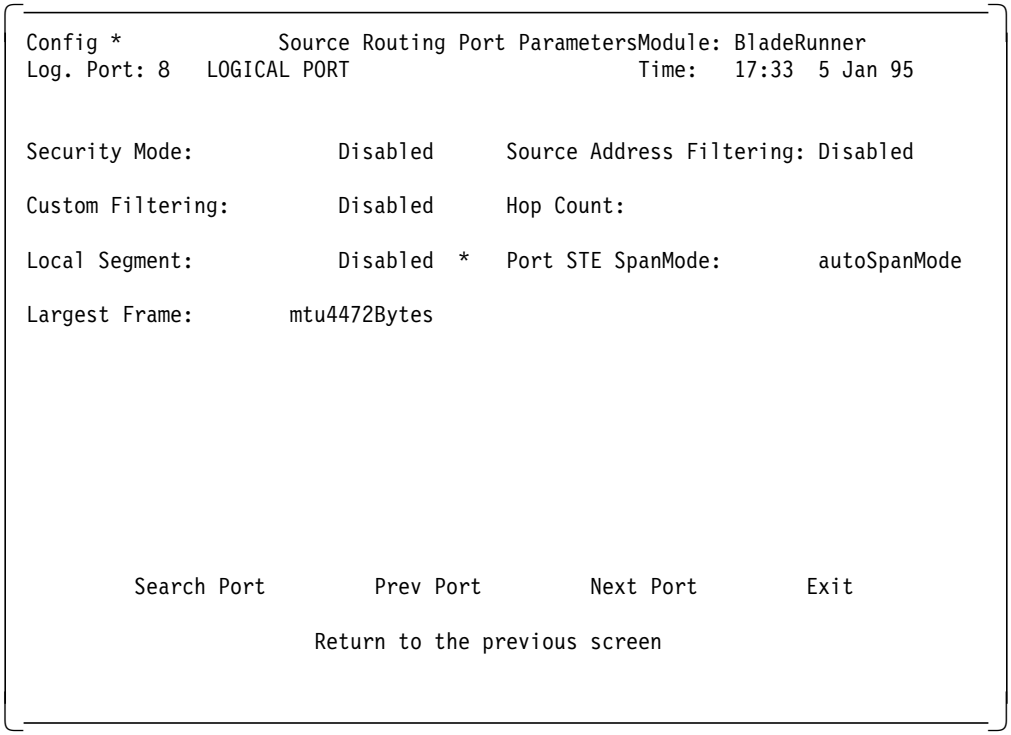


Figure 155. LMS Source Routing Port Parameter

This panel allows you to view and configure the source routing element for the selected port. This screen can only be used when a valid *bridge number* is assigned to the Multiprotocol Interconnect module. The parameters that can be configured are:

- *Hop Count*

  This parameter specifies the maximum number of hops that may be used in bridging a frame.

- *Local Segment*

  This parameter allows you to specify the segment number of the LAN to which this port is attached. If you select *disabled* for this parameter, source-route transparent bridging will be disabled on this port.

- *Largest Frame*

  This parameter specifies the maximum size of the INFO field that this port can send and receive. The valid range is 516, 1500, 2052 and 4472.

- *Port STE SpanMode*

  This parameter specifies the action to be taken on the Spanning Tree Explorer frames arriving at this port. When set to *disabled*, the port discards all such frames. *Forced* means that these frames are accepted and processed by the port. *Auto-span* means that the frames are only forwarded when the port is in *forwarding* state.

All the other parameters on this panel are identical to the parameters discussed for the *Transparent Bridging Port Parameters*.

4. Configure the *STP System Parameters* as described for in 11.8.4.1, “Configuring for Transparent Bridging” on page 262.

5. Configure the *STP Port Parameters* for each token-ring port performing source-route transparent bridging, as described in 11.8.4.1, “Configuring for Transparent Bridging” on page 262.
6. Optionally, you may configure the security and filtering parameters as described in 11.8.5, “Filtering for Bridging Functions” on page 270.

11.8.4.3 Configuring for Translational Bridging

To perform translational bridging between the token-ring and Ethernet ports attached to the Multiprotocol Interconnect module, both the token-ring and Ethernet ports must be configured for transparent bridging.

Note

If the token-ring port is enabled for source route transparent bridging, the Multiprotocol Interconnect module cannot perform translational bridging for that port.

To configure for translational bridging, you must first configure the Multiprotocol Interconnect module for transparent bridging as described in 11.8.4.1, “Configuring for Transparent Bridging” on page 262. Then, you must perform the following additional steps:

1. Select *Conversion System Parameter*. A panel as shown in Figure 156 will be displayed.

```
Config *             Conversion System Parameters  Module: BladeRunner
System                                             Time:   18:11  5 Jan 95


SNAP Conversion:   Disabled             IPX Conversion:         Enabled

                                        Exit

                          Return to the previous screen
```

Figure 156. LMS Conversion System Parameters Panel

This panel allows you to enable the translational bridging between token-ring and Ethernet ports. The following parameters can be specified on this panel:

- *SNAP Conversion*

This parameter allows you to enable/disable SNAP conversion between token-ring and Ethernet frames. When enabled, the Ethernet network is treated as an 802.3 network. When disabled, the Ethernet network is treated as an Ethernet V2 network. Note that the implication of this parameter is that the Ethernet ports can be either Ethernet V2 or 802.3 but not both.

- *IPX Conversion*

  When *enabled*, IPX packets are recognized and processed by the module for bridging between token-ring and Ethernet. If disabled, problems may arise when IPX stations try to pass data from Ethernet to token-ring networks.

11.8.5 Filtering for Bridging Functions

When performing transparent bridging (for both TB and SRT) the Multiprotocol Interconnect module will always use its filtering database to forward or discard the frames that it receives on each of its TB or SRT (for transparent bridging part only) ports. Additionally, via configuration parameters, you can define the following filtering options for each port:

- Normal or security mode for each TB port and TB part of SRT ports
- Broadcast/multicast filtering for TB ports and TB part of SRT ports
- Custom filtering for any bridging port regardless of the bridging type configured for that port

These filtering options allow you to forward or discard frames based on one or more filters strung together. If the frame matches the specified filtering criteria, it may be either discarded or forwarded with a specified priority. The following sections describe the details of various filtering options provided by the Multiprotocol Interconnect module.

11.8.5.1 Transparent Bridging Filtering Database

The Multiprotocol Interconnect module provides a global filtering database to support all the interfaces on the module using transparent bridging and the transparent bridging part of the source-route transparent bridging. This database is used to determine which frames are to be forwarded and which frames are to be discarded by the bridging function in the Multiprotocol Interconnect module.

This table is updated automatically as new addresses are *learned* by the Multiprotocol Interconnect module. You can also configure the filtering database with *permanent* entries.

The contents of the filtering database can be displayed by selecting *Filtering Database* from the *Bridge Menu*. Figure 157 on page 271 shows an example to the filtering database which is displayed.

```
Config *               Filtering Database          Module: BladeRunner
System                           Page 1            Time:   14:27  6 Jan 95

 MAC Address  Disposition  Scope         MAC Address  Disposition  Scope

#0000B528023E 1            all          %090077000002
%0180C2000000
#08005A1326EB 2            all
%08008F4001A0
%08008F4001A1
%08008F4001A2
%08008F4001A3
%08008F4001A4
%08008F4001A5
%08008F4001A6
%08008F4001A7
%090077000001
+ Unlearned    # Learned    * Static    $ Permanent    % Management


Add Entry    Freeze Database    Search Addr    Prev Page    Next Page

                        Return to the previous screen
```

Figure 157. LMS Configuration Panel

Entries in the filtering database consist of:

- *MAC Address*

  These are the addresses that have been learned dynamically by the Multiprotocol Interconnect module as well as fixed addresses that are entered by the user manually.

- *Scope*

  This field indicates the ports to which this entry applies, that is, the ports that can forward frames to this MAC address. The value of the scope can be a specific *port number* or *all*. All learned entries have a scope of *all*.

- *Disposition*

  This field specifies the action to be taken when a frame with a destination address matching this MAC address is received. The values for disposition can be a *port number* to which the frame will be forwarded or *flood* which means forwarding to all the bridge ports or *discard* which means the frame is not to be forwarded on any port. Note that disposition for learned entries is the port number on which the station was learned.

  In front of each MAC entry there is a sign which has the following meaning:

  – *Unlearned (+)*

    This entry was learned but has been aged-out. Aged out entries will not be used for frame forwarding or discarding. They remain in the database to provide historical information about the MAC addresses learned on each port.

  – *Learned (#)*

    This entry has been learned automatically by the Multiprotocol Interconnect module.

– *Permanent($)*

  These are manually entered addresses which are stored in the FLASH memory.

– *Static (*)*

  These are entries that have been entered manually. They cannot be aged-out of the filtering database, but will be lost during a module *Reset*. Usually the manually entered addresses are permanent and are retained in the FLASH memory which results in them being retained during the module reset. But, if the FLASH is too full to store the address, that address becomes static.

– *Management(%)*

  These addresses are internal addresses used by the Multiprotocol Interconnect module and cannot be altered. They include addresses used by the Hello BPDU of the spanning tree protocol as well as the MAC addresses of the LAN ports.

To add a permanent or static entry to the filtering database, select *Add Entry* from this panel. You will then be allowed to enter the following via a pop-up panel:

- MAC address
- Disposition
- Scope

Permanent or static entries from the filtering database can be deleted using the *Delete Entry* option on this panel.

The *Freeze Database* option allows you to freeze the filtering database and make all the entries either permanent (if there is space in FLASH) or static. Once the database is frozen, no new entries may be learned, and no entries may be added, deleted, or forgotten.

The Multiprotocol Interconnect module will add addresses to the filtering database under the following conditions:

1. *Bridging* is enabled for the module
2. *Source Address Learning* is enabled for the receiving port
3. The receiving port is in *forwarding* or *learning state*
4. The source address is a unicast address
5. A fixed entry for the address does not already exist
6. There is space in the database. If the database is full, the Multiprotocol Interconnect module will try to find an entry for which its time-to-forget has expired. If such an entry is found, it is deleted and the new address is learned (added to the database). If there is no room in the database and a *forgotten* entry is not found the address is not learned.

The learned addresses are not kept in the filtering database forever. The Multiprotocol Interconnect module keeps track of each learned entry in the filtering database and deletes it when it has not been used for a specified length of time. This process keeps the database up-to-date and prevents it from running out of space.

To do this, each address in the database has an age assigned to it. When the address is learned, the age is set to zero. At subsequent time intervals this address is incremented. There are two system-wide timers which govern the length of the time the learned entries will be kept in the filtering database:

- *Time-to-Forget*

  If an address is already in the filtering database and no packets are received from this source by the Multiprotocol Interconnect module within the time-to-forget interval, then the address is marked as *forgotten*. Forgotten entries are no longer used for filtering purposes. They remain in the filtering database for historical information, until the time-to-delete period expires.

- *Time-to-Delete*

  After an address is marked as *forgotten*, this parameter determines the length of the time the entry may remain in memory without being relearned. If this time expires before any packets are received from the module, the entry is deleted from the filtering database.

Time-to-forget and time-to-delete are system-wide parameters and can be set by the user using the *Bridge System Parameters* panel.

11.8.5.2 Operating Modes for Bridging Ports

Each port of the Multiprotocol Interconnect module which is configured for bridging (TB or SRT) can operate in one of the following two modes:

1. *Normal Mode*

   In this mode the port can perform the following functions:

   - Can learn new addresses if *Source Address Learning* is enabled for that port
   - Can forward/filter frames
   - Can communicate with network management software
   - Will participate in spanning tree protocol

2. *Security Mode*

   In this mode the port can perform the following functions:

   - Can learn new addresses if *Source Address Learning* parameter for that port is enabled
   - Can forward frame if destination address is permanent or static
   - Can communicate with network management software
   - Will participate in spanning tree protocol if STP is enabled

Note that the difference between normal and security mode is that in security mode, only the frames destined to stations with permanent entry will be bridged via the port. You can use the security mode to ensure that the stations attached to a secure port can communicate with specific stations on the other LANs through the Multiprotocol Interconnect module.

The mode for each port can be set independently from the other ports. The setting of the mode is done through the LMS on the *Transparent Bridging Port Parameters* panel.

11.8.6 Destination Address Filtering

Destination address filtering allows you to use the contents of the filtering database to forward or discard frames. Destination address filtering is always performed by the Multiprotocol Interconnect module. However, certain configurable parameters as described below will affect the operation of the destination address filtering:

- If the port is operating in normal mode and the destination address of the frame is found in the filtering database, the packet is bridged according to the *disposition* specified for that MAC address (other filters permitting).
- If the port is operating in normal mode and the destination address of the frame is not found in the filtering database, the frame is sent on all the other ports (flooded) enabled for transparent bridging (other filters permitting).
- When a packet is received and the port is operating in security mode, if no static/permanent entry is found in the filtering database for the destination address of the frame, the packet is discarded. If a static/permanent entry is found, the frame will be forwarded (other filters permitting).

11.8.6.1 Source Address Filtering

Source address filtering allows you to specify the stations from which frames will be bridged. Source address filtering may be enabled/disabled for each port using the *Transparent Bridging Port Parameters* and the *Source Routing Port Parameters* panels.

If source address filtering is enabled, when a packet is received, the module searches the filtering database for the source address. If it is present (it must be permanent or static) and address disposition is the receiving port, then the packet will be forwarded (other filters permitting). Otherwise, the packet is discarded. This ensures that only the frames from predefined MAC addresses and on predefined networks will be able to communicate through the bridge.

Also, source address filtering, combined with security mode, allows you to forward only the traffic between predefined stations and on predefined networks.

11.8.6.2 Broadcast/Multicast Filtering

When the port is operating in security mode, all the broadcast/multicast frames will be discarded. However, by setting *Broadcast/Multicast Filtering* on the secure port to *Always Accept Multicast*, all broadcast and multicast traffic will be accepted from that port and forwarded to all the other ports.

Note that in normal mode with the default disposition of *flood*, the broadcast/multicast traffic is forwarded regardless of the setting of this filter.

11.8.6.3 Custom Filtering

This facility allows a number of custom tests to be applied to the received traffic to determine if the frame should be forwarded or discarded. This facility is offered on a per port basis; that is, you can perform different tests on different ports, and is applied after the standard destination address filtering (and source address filtering if enabled). Therefore, packets discarded during the destination address filtering (and source address filtering) are not subject to custom filtering.

To perform custom filtering, you must perform the following:

1. Define all the tests that you may want to be applied to the received frames by the Multiprotocol Interconnect module. This is done by creating a *Custom*

Filter Test Table. Note that there is only one of these tables in each Multiprotocol Interconnect module and it contains all the test that are to be performed by the Multiprotocol Interconnect module, regardless of the ports on which these tests are performed.

To define the tests, select *Custom Filter Test Table* from the *Bridge Menu*. An example of the panel displayed is shown in Figure 158.

```
Config *          Custom Filter Test Table        Module: BladeRunner
System                      Page 1                 Time:   14:07  9 Jan 95

ID  Test Name             Filter Start Offset   Mask   Operator       Value
1   ""                    mac          0      00000000 equal        00000000
2   ""                    mac          0      00000000 equal        00000000
3   ""                    mac          0      00000000 equal        00000000
4   ""                    mac          0      00000000 equal        00000000
5   ""                    mac          0      00000000 equal        00000000
6   ""                    mac          0      00000000 equal        00000000
7   ""                    mac          0      00000000 equal        00000000
8   ""                    mac          0      00000000 equal        00000000
9   ""                    mac          0      00000000 equal        00000000
10  ""                    mac          0      00000000 equal        00000000
11  ""                    mac          0      00000000 equal        00000000
12  ""                    mac          0      00000000 equal        00000000




  Modify Entry          Prev Page             Next Page             Exit

                     Return to the previous screen
```

Figure 158. LMS Custom Filter Test Table Panel

This table may have up to 64 entries. You may define the following parameters for each entry:

- *ID Number*

  This number is used to refer to this test from the other filtering tables.

- *Test Name*:

  This is a meaningful name assigned to the test and used to refer to this test from the other filtering tables.

- *Filter Start Point*

  This field is used to select either MAC header, LLC header or length of the frame as the starting point for the offset into the frame.

- *Offset*

  This field represents the number of bytes from the *Filter Start Point* within the frame where the test is to apply. The test can start anywhere within the first 65,536 bytes of a frame.

  Note: When frame_length is specified as the filter start point, the offset is not applied.

- *Mask*

This field defines the bits in the received frame, starting at the specified *offset*, that should be tested against the contents of the *value* field. Only the bits which have a value of B′1′ in the mask will be tested.

- *Logical Operator*

  The following operators can be used for testing:

  - Equal
  - Not_equal
  - Less_than
  - Greater_than

- *Value*

  This field specifies the 32-bit unsigned value against which the contents of a frame starting at the specified *offset* should be compared.

When you install the Multiprotocol Interconnect module (or after a cold start), the custom filter test table has 64 dummy entries defined for it. To define a test, select the *Modify Entry* parameter on this panel. A pop up window will be displayed, which allows you to define the parameters described above. Once the entry is defined, select *Set Entry* to confirm or *Cancel* to abandon the operation. An example of a Custom Filter Test Table entry is shown in Table 39.

Table 39. Custom Filter Test Table

ID	Test Name	Filter Start	Offset	Mask	Operator	Value
1	802.3	MAC	12	FFFF0000	<	05DC

This example enables the Multiprotocol Interconnect module to test the contents of two bytes, starting at offset 12 from the beginning of the MAC address against the value X′5DC′ (1500 decimal). In Ethernet frames, this is called the ″length″ or ″type″ field. In Ethernet V2 frames, this field always contains a value higher than 1500, whereas 802.3 frames always contain a value less than 1500. Therefore, this entry allows you to check and see if the frame is an 802.3 or Ethernet V2 frame.

2. Once you have defined all the desired tests, you must define the tests that should be performed on each port, using the *Custom Filter Statement Table*. Note that there is one Custom Filter Statement Table for each port.

   To define entries in the Custom Filter Statement Table, select **Custom Filter Statement Table** from the *Bridge menu*. An example of this table is shown in Figure 159 on page 277.

```
Config *        Custom Filter Statement Table      Module: BladeRunner
Log. Port: 1   LOGICAL PORT     Page 1             Time:   14:10  9 Jan 95

Statement ID Test Name          Action on Success     Action on Failure
1           Frame Type Test       Stmt 2                Discard
2           ""                    Discard               Discard
3           ""                    Discard               Discard
4           ""                    Discard               Discard
5           ""                    Discard               Discard
6           ""                    Discard               Discard
7           ""                    Discard               Discard
8           ""                    Discard               Discard
9           ""                    Discard               Discard
10          ""                    Discard               Discard









Modify Entry     Prev Page     Next Page     Prev Port     Next Port     Exit

                        Return to the previous screen
```

Figure 159. LMS Custom Filter Statement Table

The port to which the table applies is displayed on the top left hand corner of the screen. You can use the *Prev Port* and *Next Port* options on the Menu Bar to select the required port.

This table allows you to apply up to 16 tests on the frames received on each port.

To configure a new entry in the table, you must select *Modify Entry* and type the entry's *Statement ID*. Once you have entered the information for the entry, you must select **Set Entry** and press Enter to confirm or select *Cancel* to abandon the operation. The following parameters can be specified for each entry in the Custom Filter Statement Table:

- *ID Number*

  This is the number assigned to the selected test in the *Custom Filter Test Table*.

- *Test Name*:

  This is the name assigned to the selected test in the *Custom Filter Test Table*.

- *Action on Success*

  This parameter specifies the action to be taken by the Multiprotocol Interconnect module when the test is successful.

- *Action on Failure*

  This parameter specifies the action to be taken by the Multiprotocol Interconnect module when the test is unsuccessful.

  For both the *Action on Success* and *Action on Failure*, the following values can be specified:

  – Discard: Discard the frame

- Fwd Prio #: Forward the frame at the specified priority (#). # can be 0 to 7. Priority 0 is the highest priority.
- Stmt #: Specifies another statement ID from the Custom Filter Statement Table, so that another test may be applied to the frame. # can be 1 to 16.

An example of the use of priority is to check for the frame size and assign higher priority for shorter frames (typically interactive sessions) over the longer frames (typically batch/file transfer sessions).

An example of a Custom Filter Statement Table entry is shown in Table 40.

Table 40. Custom Filter Statement Table

ID	Test Name	Action on Success	Action on Failure
1	802.3	Forward	Discard

3. Once the you have defined all the entries for all the ports, you must enable the *Custom Filtering* option for each port on which you want to apply the specified test. The Custom Filtering option is specified on the *Transparent Bridging Port Parameters* and *Source Routing Bridging Port Parameters* panels.

11.8.7 Configuring for Routing Functions

To configure the Multiprotocol Interconnect module for routing, you must select the *Protocols Menu* from the *Configuration Menu*. This panel allows you to display and modify the configuration parameters relevant to the routing functions of the Multiprotocol Interconnect module. The Protocols Menu panel is shown in Figure 160.

```
Config *                          Protocols Menu    Module: BladeRunner
                                                    Time:   15:17  9 Jan 95


                                    IP

                                    OSPF

                                    DECnet IV

                                    IPX

                                    Exit









                          Return to the previous screen
```

Figure 160. LMS Protocols Menu Panel

The following sections describe the procedures used to configure the Multiprotocol Interconnect module to perform one of the following:

- IP routing
- IPX routing
- DECnet Phase IV routing

11.8.8 Configuring for IP Routing

The Multiprotocol Interconnect module allows you to use RIP, OSPF, and static routes when used as an IP router.

To configure the Multiprotocol Interconnect module as an IP router you must do the following:

1. Configure the system-wide parameters for the Multiprotocol Interconnect module as described in 11.8.1, “Configuring System Wide Parameters” on page 252.
2. Configure the port parameters for the Multiprotocol Interconnect module’s ports as described in 11.8.2, “Configuring Port Parameters” on page 255.
3. Select *IP* from the *Protocols Menu*. A panel as shown in Figure 161 will be displayed:

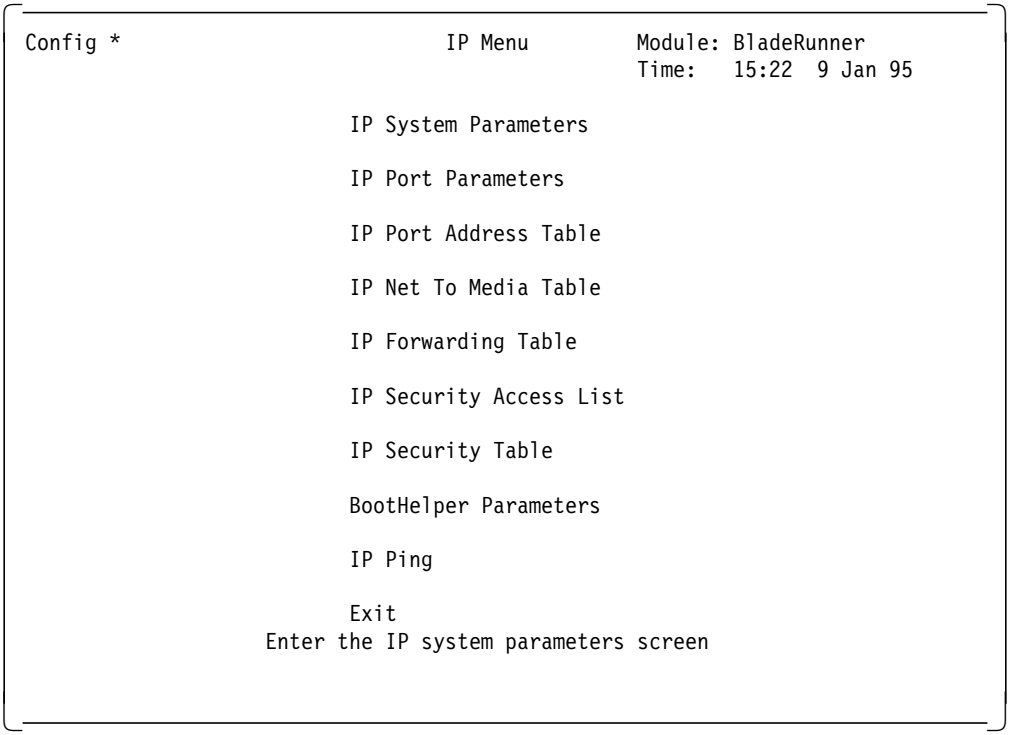


Figure 161. LMS IP Panel

This screen allows you to access all the IP configurable parameters supported by the Multiprotocol Interconnect module.

4. Assign IP addresses to the ports that must perform IP routing. To do so, select *IP Port Address Table* from the *IP Menu*. An example of this panel is shown in Figure 162 on page 280.

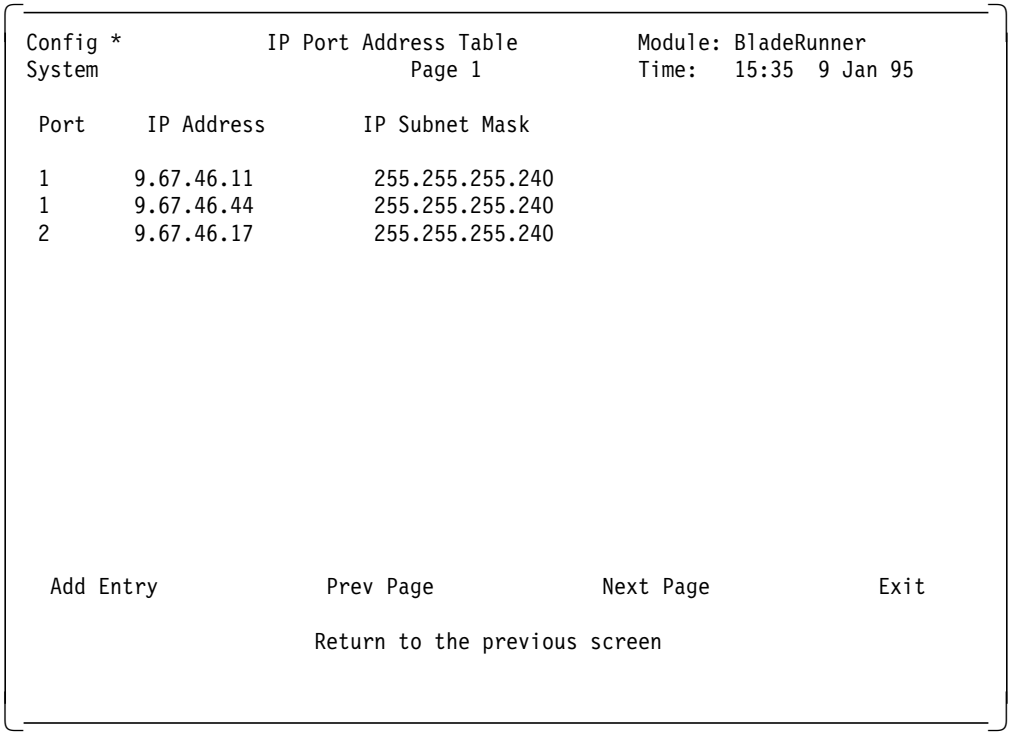


Figure 162. LMS IP Port Address Table Panel

This table allows you to view and/or modify the IP addresses assigned to each port.

The Multiprotocol Interconnect module allows you to configure up to five IP addresses for each LAN port. This is a useful feature that can be used in the following situations:

- There are too many hosts on a LAN to be accommodated in a single IP subnetwork.
- Two separate IP subnetworks have been bridged together and you want to use a single port on this module to route the traffic from these bridged networks.

You must take the following into consideration when assigning IP addresses to the ports:

- Only one port per subnetwork is allowed
- The same IP address may not be assigned to more than one port
- IP broadcast address may not be assigned to a port
- If port does not have an IP address, IP routing cannot be enabled on that port
- If no IP address is assigned to any of the ports, the IP routing function cannot be enabled at the module level
- The Multiprotocol Interconnect module can send and receive BOOTP messages on a port with no configured IP address

5. Enable IP routing globally for the module. To do so, you must select *IP system Parameters* from the *IP Menu*.

   Note: If you try to enable IP for the module, before assigning an IP address to at least one port, your request will be rejected.

An example of the IP System Parameters panel is shown in Figure 163 on page 281.

```
Config *            IP System Parameters          Module: BladeRunner
System                                            Time:   15:43  9 Jan 95

IP Routing:  Enabled

RIP:         Enabled                  Router ID:          9.67.46.44

IP Security: Disabled

ARP Timeout: 1500                     Reassembly Timeout: 10

Proxy ARP:   Disabled                 Source Quench:      Disabled

Redirect:    Disabled                 ICMP tx rate:       1000

Hash Size:   512                      Default TTL:        16



                                    Exit

                        Return to the previous screen
```

Figure 163. LMS IP System Parameters Panel

This panel allows you to display and modify the system-wide IP parameters. The parameters that can be viewed and/or configured are:

- *IP Routing*

  This parameter allows you to enable IP routing throughout the module. Note that IP routing for each port participating in IP routing should also be enabled in order for those ports to perform IP routing.

- *RIP*

  This parameter controls whether RIP is enabled or disabled throughout the module.

- *Router ID*

  This parameter is used on WAN interfaces that have no assigned IP address. You may configure any one of the IP addresses assigned to the interfaces on the module as the Router ID.

- *IP Security*

  This parameter enables/disables the operation of the IP security feature on the Multiprotocol Interconnect module. The IP security is a filtering facility and is described in 11.8.9, “IP Security” on page 304.

- *ARP timeout*

  This parameter specifies the length of time (in minutes) that an idle entry may remain in the ARP (Address Resolution Protocol) table. If set to 0, no aging is performed. If the ARP table is full, no new addresses are learned.

- *Reassembly timeout*

This parameter specifies the length of time that the module may wait for all the fragments of a fragmented IP message to be received for reassembly. If they are not received within the specified time, the datagram is discarded. Note that datagram reassembly takes place at the destination of a datagram only.

- *Proxy ARP*

  If the module receives an ARP request for a host whose network or subnetwork address is assigned to one of its ports or if the module knows a route to the host, the module sends an ARP reply containing its own MAC address. Subsequently, all the packets directed to that host will be sent to the Multiprotocol Interconnect module which will in turn forward them to the correct destination.

- *Source Quench*

  This parameter specifies if the module generates ICMP source quench messages. These messages are sent to hosts, requesting them to reduce their data transmission rate.

- *Redirect*

  This parameter specifies if the module generates ICMP redirect messages. These messages are sent when the Multiprotocol Interconnect module recognizes that the sender of the IP packet is not using the optimal route to the destination. These messages are sent to the source of the frame, informing it of the faster route. The Multiprotocol Interconnect module processes received ICMP redirect messages and adds the routes to its IP routing table.

- *ICMP tx Rate*

  This parameter controls the rate at which ICMP messages are generated.

- *Hash Size*

  This parameter controls the hash size for the IP routing table.

- *Default TTL*

  This parameter specifies the value that is inserted into the *time-to-live* field of the IP datagrams originated on this module, whenever the value is not supplied by the transport protocol.

6. Enable IP routing on each port which is to perform IP routing. To do so, select *IP Port Parameters* from the *IP Menu*. An example of the IP port parameter panel is shown in Figure 164 on page 283.

```
Config *              IP Port Parameters            Module: BladeRunner
Log. Port: 1   LOGICAL PORT                         Time:   15:55  9 Jan 95

IP Port Routing:        Enabled         Disposition:            discard

RIP:                    Enabled  *      IP Mtu:                 1492

RIP Path Cost:          1              LAN Encapsulation:      ethernet

Broadcast Form:         ones           Forward Broadcast:      Enabled

Security Access List 1: 0              Security Access List 2: 0









        Search Port         Prev Port         Next Port         Exit

                       Return to the previous screen
```

Figure 164. LMS IP Port Parameter Panel

This panel allows you to display and configure IP parameters for each logical port. The following parameters can be specified on this panel:

- *IP Routing*

  This parameter allows you to enable IP routing for each port. Note that to perform IP routing, IP routing must be enabled at both the module and port level.

- *Disposition*

  This parameter is valid if the IP routing is disabled at the port level but enabled at the module level. It specifies if the IP traffic received at the port level is bridged or discarded.

- *RIP*

  This parameter controls whether RIP is enabled or disabled for this port.

- *IP Mtu*

  This parameter specifies the maximum size of the IP packets that may be transmitted on this port.

- *RIP Path Cost*

  This parameter specifies the RIP path cost assigned to this logical port.

- *LAN Encapsulation*

  This parameter specifies the LAN encapsulation used to transmit a datagram on this port. Note that for Ethernet connections you can choose Ethernet or 802.3 but not both.

- *Broadcast Form*

  This parameter specifies which form of broadcast (all 0′s or all 1′s) is used by the module to send broadcast messages on this interface. Note

that the Multiprotocol Interconnect module recognizes both types of broadcasts on the received frames regardless of the setting of this parameter.

- *Forward Broadcast*

  This parameter specifies if this port will forward directed broadcast messages. Directed broadcasts have all 1′s in the *hostid* portion of their address.

- *Security Access List n*

  This parameter specifies the security access list associated with this port. You may assign two security access lists with a single logical port. IP security must be enabled at the module level for the security feature to be active. Note that a value of 0 indicates that this list is inactive. For more information about IP security, refer to 11.8.9, “IP Security” on page 304.

7. Optionally, you may specify one or more *static routes* to be used by the Multiprotocol Interconnect module. To do so you must select *IP Forwarding Table* from the *IP menu*. An example of the IP forwarding table is shown in Figure 165.

```
Config *              IP Forwarding Table          Module: BladeRunner
System                          Page 1             Time:   16:08  9 Jan 95

 Destination      Next Hop        Mask          Type     Port Protocol Metric1

9.67.46.0       0.0.0.0         255.255.255.240 local     1   local     1
9.67.46.16      0.0.0.0         255.255.255.240 local     2   local     1
9.67.46.32      0.0.0.0         255.255.255.240 local     1   local     1
9.67.46.224     9.67.46.46      255.255.255.240 remote    1   netmgmt   1

 Add Entry         Search Addr        Prev Page        Next Page        Exit

                      Return to the previous screen
```

Figure 165. LMS IP Forwarding Table Panel

This table allows you to create static routes which can be used by the Multiprotocol Interconnect module to determine on which port each datagram should be transmitted. It also allows you to display the current routing tables used by the Multiprotocol Interconnect module. The following entries can be viewed/modified using this table:

- *Destination*

  This field can be either a host address, a subnet address, or a network address.

- *Next Hop*

  This is the IP address of the node that is the next stop for a packet en route to its destination address. The next hop must be directly connected to the interface for which this route is defined.

- *Mask*

  This is the subnet mask associated with the destination address entry.

- *Type*

  This field indicates whether the destination address is directly connected to this interface. The valid values are:

  – Direct

  – Indirect

  – Other

  – Invalid

- *Port*

  This field specifies the logical port on which the packets should be forwarded.

- *Protocol*

  This is a read-only field indicating whether the route has been statically configured or learned by one of the routing protocols including ICMP.

- *Metric*

  This field indicates the cost of the route to its destination. A value of 16 means unreachable.

Note that in the example given above, the last entry is a static route added to the table whereas the other three entries are automatically learned by the Multiprotocol Interconnect module.

8. Optionally, you may specify one or more entries in the ARP table to be used by the Multiprotocol Interconnect module to resolve IP addresses to the correct MAC address. To do so, you must select *IP Net To Media Table* from the *IP Menu*. An example of the resulting panel is shown in Figure 166 on page 286.

```
Config *            IP Net To Media Table          Module: BladeRunner
System                        Page 1               Time:   10:50 11 Jan 95

Port    Network Address    Media Address     Type

 1      9.67.46.13         400000000001      static
 1      9.67.46.33         10005A7903C7      dynamic
 1      9.67.46.34         10005A7903E1      dynamic
 1      9.67.46.40         0000B528023E      dynamic
 1      9.67.46.41         08008F3003EF      dynamic
 1      9.67.46.46         08005A13396F      dynamic









 Add Entry         Search Addr        Prev Page        Next Page        Exit

                Add a new entry to the IP Net To Media Table
```

Figure 166. LMS IP Net To Media Table

This table can be used to view and/or modify the contents of the ARP table. Each entry in this table contains the following parameters:

- *Network Address*

  This parameter specifies the IP address of the station that this entry applies to.

- *Physical Address*

  This parameter specifies the MAC address of the station that this entry applies to.

- *Type*

  This field is a read-only field and indicates that the address mapping has been learned through ARP (dynamic) or configured by the user (static).

To add a static entry to the ARP table, select *Add Entry* from this panel. A pop-up menu will be displayed which allows you to enter the IP address and the corresponding MAC address. Once, you have specified this information select *Set Entry* to add the entry to the ARP table or *Cancel* to abandon the operation.

9. If you are planning to use the BOOTP protocol between a BOOTP server and client and the BOOTP client is connected to the BOOTP server via the Multiprotocol Interconnect module, you must configure your module as a *Boothelper*.

   BOOTP allows a client to request the following from a BOOTP server:

   - Client's own IP address
   - IP address of a TFTP server
   - Name of the code image file

Also a BOOTP client can request the code image file to be downloaded from the TFTP server.

To configure the Multiprotocol Interconnect module as a Boothelper you must select *Boothelper Parameter* from the *Protocols Menu*. An example of the Boothelper Parameters panel is shown in Figure 167.

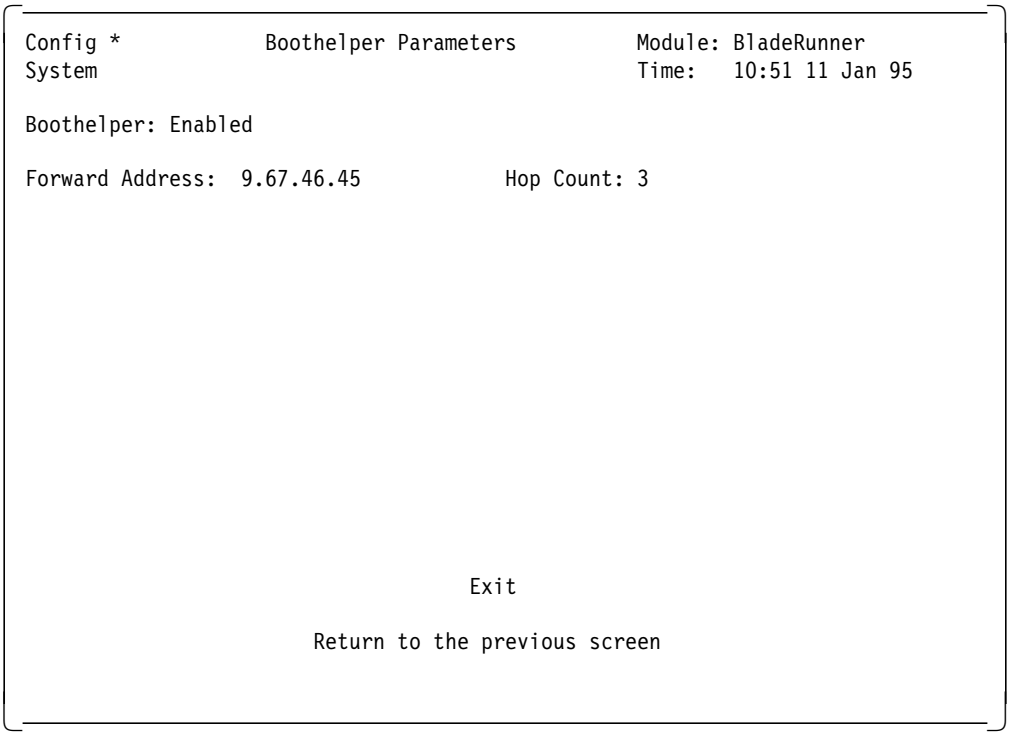


Figure 167. LMS Boothelper Parameters Panel

This screen allows you to display and configure module-wide Boothelper parameters for the Multiprotocol Interconnect module. The following parameters can be specified using this panel:

- *Boothelper*

  If this parameter is disabled, all the BOOTP datagrams are discarded by the Multiprotocol Interconnect module. If enabled, they will be forwarded to the address specified by *Forward Address* parameter.

- *Forward Address*

  This is either the IP address of the BOOTP server (if the BOOTP server is directly connected to the module) or the IP address of the next Boothelper router in the path to the BOOTP server.

- *Hop Count*

  This parameter restricts the number of Boothelpers that BOOTP messages may traverse before reaching the BOOTP server. The message will be discarded if the number of hops is equal to or exceeds the value configured for this parameter.

In this example, the station with IP address 9.67.46.45 is an RS/6000 workstation configured as a BOOTP server.

10. If you are planning to use OSPF, you must configure the Multiprotocol Interconnect module for OSPF as described in the following section.

11.8.8.1 Configuring for OSPF

To configure the Multiprotocol Interconnect module to use OSPF, you must select *OSPF* from the *Protocols Menu*. The resulting panel is shown in Figure 168.

```
Config *                          OSPF Menu       Module: BladeRunner
                                                  Time:   11:11 11 Jan 95

                              OSPF System Parameters
                              OSPF Area Table
                              OSPF Area Default Metric Table
                              OSPF Address Range Table
                              OSPF Host Table
                              OSPF Interface Table
                              OSPF Interface Metric Table
                              OSPF Virtual Interface Table
                              OSPF Neighbor Table
                              OSPF RIP Filter Table
                              OSPF RIP Convert Table
                              OSPF RIP Default Convert Table
                              OSPF Static Filter Table
                              OSPF Static Convert Table
                              OSPF Static Default Convert Table
                              Exit


                    Enter the OSPF system parameters screen
```

Figure 168. LMS OSPF Menu Panel

This menu panel allows you to access all the panels related to viewing and configuring OSPF parameters for the Multiprotocol Interconnect module. The following steps should be taken to configure the various parameters required by OSPF:

1. Configure the system-wide OSPF parameters by selecting *OSPF System Parameters* from the *OSPF Menu*. An example of the OSPF System Parameters panel is shown in Figure 169 on page 289.

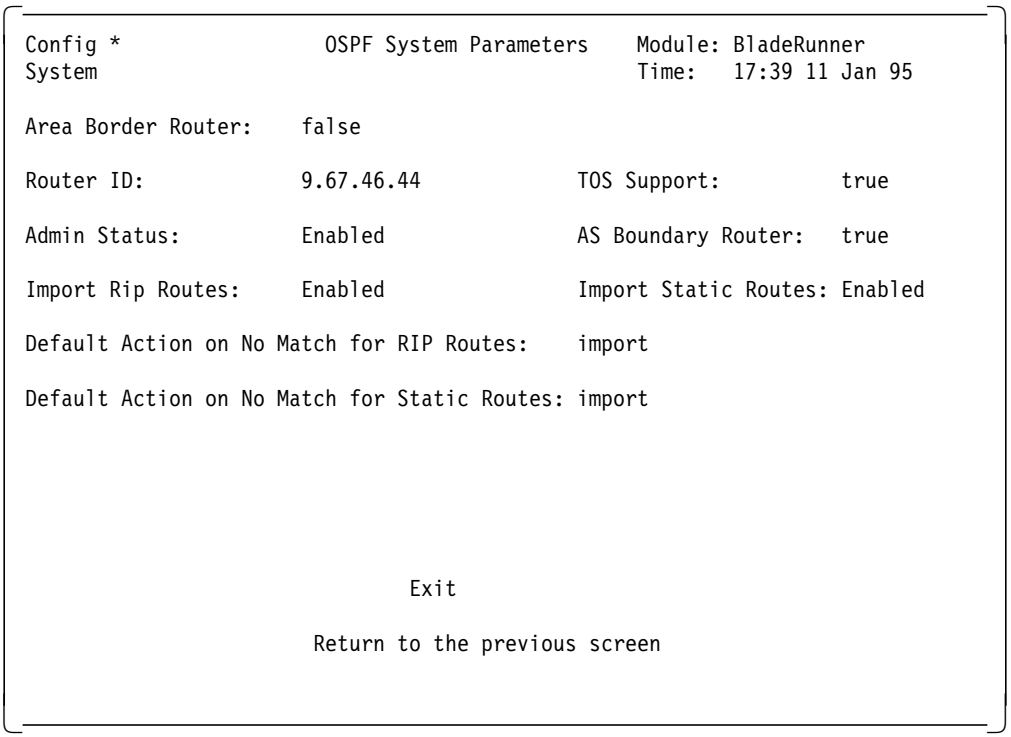


Figure 169. LMS OSPF System Parameter Panel

This panel allows you to display and configure the system-wide OSPF parameters.

- *Area Border Router*

  This parameter is a read-only parameter and tells you if the router is an Area Border router.

- *Router ID*

  This is the IP address that uniquely identifies this router. It can be any valid IP address assigned to an interface on this module. The router ID will determine the designated router on a broadcast link if the priority values of the routers being considered are equal. The higher the router ID, the greater its priority.

- *TOS Support*

  This parameter specifies if the Type Of Service (TOS) routing is enabled on this module.

- *Admin Status*

  This parameter allows you to enable/disable OSPF routing throughout the module. If OSPF is disabled on this panel, then it is disabled on each port.

- *AS Boundary Router*

  If this router is an AS Boundary router, set this parameter to true. A router can be an AS boundary router if one or more of its interfaces is connected to a non-OSPF network (for example RIP).

- *Import RIP Routes*

This parameter determines if the RIP filter table will be used for importing routes found by RIP. RIP filter table is discussed later in this section.

- *Import Static Routes*

  This parameter determines if the static route filter table will be used for importing static routes. Static route filter table is discussed later in this section.

- *Default Action on No Match for RIP Routes*

  This parameter specifies the action to be taken when a RIP route does not match any entry in the RIP filter table. If this parameter is set to *import*, a route found by RIP that does not have a match in the RIP filter table is imported using the default hop-to-metric conversion table. Otherwise, it is not imported. Hop-to-metric conversion table is explained later in this section.

- *Default Action on No Match for Static Routes*

  This parameter specifies the action to be taken when a static route does not match any entry in the static route filter table. If this parameter is set to *import*, a static route that does not have a match in the static route filter table is imported using the default hop-to-metric conversion table. Otherwise, it is not imported.

2. Define the interfaces that are enabled for OSPF. To do so, you must select *OSPF Interface Table* from the *OSPF Menu*. An example of the resulting panel is shown in Figure 170.

```
Config *              OSPF Interface Table         Module: BladeRunner
System                          Page 1             Time:   17:40 11 Jan 95

IP Address      Port   Area ID         Type          AdminStat Priority PollInt

9.67.46.17      0      0.0.0.0         broadcast     Disabled  1        120
9.67.46.44      0      0.0.0.0         broadcast     Enabled   1        120
9.67.46.94      0      0.0.0.0         broadcast     Disabled  1        120

                Modify Entry     Prev Page        Next Page       Exit

                        Return to the previous screen
```

Figure 170. LMS OSPF Interface Table Panel

This table allows you to specify the OSPF-specific information about the interfaces. Note that you cannot create or delete entries on this table. They

can only be modified. There will be one entry in this table for each IP address assigned to the Multiprotocol Interconnect module's ports.

To modify the parameters on this panel, you must select the *Modify Entry* option. A pop-up menu will be displayed which allows you to change the following parameters for each IP interface:

- *IP Address*

  This parameter specifies the IP address of the port. This parameter must be one of the IP addresses currently displayed on the panel.

- *Port*

  This parameter specifies the port number associated with this interface.

- *Area ID*

  This parameter specifies the *area* to which the port connects.

- *Type*

  This parameter specifies the type of network to which the interface is connected. The choices are:

  – *broadcast*

    Broadcast networks such as TR and Ethernet LANs

  – *nbma*

    Non-broadcast multi-access networks such as X.25 and Frame Relay

  – *PointToPoint*

    Point-to-Point links

- *AdminStat*

  This parameter enables/disables OSPF on this port. Note that OSPF should also be enabled at the module level for the port to use OSPF. When disabled, the interface is external to OSPF.

- *Priority*

  This parameter specifies the priority of this interface. In a multi-access network, this parameter is used for *designated router* selection. A value of 0 indicates that the router is not eligible to become designated router on this particular network. In the event of a tie, the router ID will be used as a tie breaker.

- *Trans Delay*

  This field specifies the estimated number of seconds it takes to transmit a packet over this interface.

- *RetranInt*

  This field specifies the length of time in seconds between link-state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting OSPF packets.

- *HelloInt*

  This parameter specifies the frequency with which the OSPF Hello packets are sent on this interface.

- *PollInt*

This parameter specifies the number of seconds between the Hello Packets that the router sends on the interface. This interval must be the same for all the routers attached to the same network.

- *RtdDeadInt*

  If a router's neighbor does not see a Hello packet within this period, it will declare the router down. The Dead Interval should be some multiple of the Hello Interval.

- *AuthKey*

  This is the character string that will be exchanged between the routers to perform partner authentication.

Also, note that if you select an entry in this table and press the *Enter* key, the following additional information about that entry can be displayed:

- *TransDelay*

  See above for the description of this parameter.

- *ReTransInt*

  See above for the description of this parameter.

- *RtsDeadInt*

  See above for the description of this parameter.

- *HelloInt*

  See above for the description of this parameter.

- *Events*

  This parameter specifies the number of times that this interface has changed state or an error has occurred.

- *IfState*

  This field displays the state of this interface. The possible states are:

  – down
  – waiting
  – pontToPoint
  – designatedRouter
  – backupdesignatedRouter
  – otherDesignatedRouter

- *Designated Router*

  This field displays the address of the designated router.

- *Backup Designated Router*

  This field displays the IP address of the backup designated router.

- *Events*

3. Define the OPSF *Areas* to which this module is attached. To do so, you must select *OSPF Area Table* entry from the *OSPF Menu*. An example of the resulting panel is shown in Figure 171 on page 293.

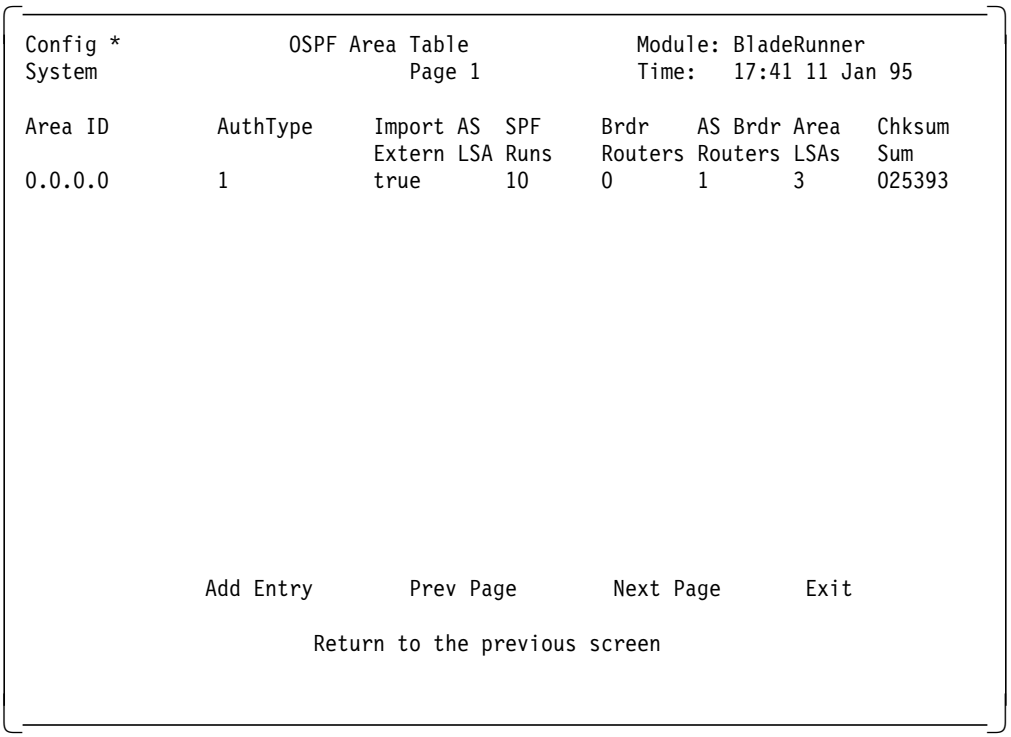


Figure 171. LMS OSPF Area Table Panel

This table contains information regarding the various areas in the AS. The following parameters can be viewed and/or modified in this table:

- *Area ID*

  This parameter uniquely identifies the area.

- *Auth Type*

  This parameter identifies the authentication type to be used for this area. The choices are 0 (no authentication) and 1 (simple password). With simple password chosen, only those routers sharing the correct password will be able to communicate with each other. If you choose simple password when you configure the interface, you will be prompted for the area password.

- *Import AS Extern LSA*

  This parameter specifies if importing AS external link state advertisements is supported by this area. If this area does not import AS external link state advertisements, it is a stub area.

- *SPF Runs*

  This is a read-only parameter and shows the number of times the intra-area route table has been calculated.

- *Brdr Router*

  This parameter is read-only and shows the total number of AS border routers reachable within this area.

- *Area LSAs*

  This parameter is read-only and indicates the total number of link state advertisements in this area's database.

- *Chksum Sum*

This parameter is read-only and contains 32-bit unsigned sum of the Link-state-advertisement's link-state checksum contained in this area's link-state database. This sum can be used to determine if there has been a change in a router's link-state database and to compare the link-state database of two routers.

Note: Area 0.0.0.0, by definition, is the backbone area and is always present in the OSPF area table.

4. When an area border router is connected to a stub area, it generates a default link summary into the area, indicating a default route. You can specify the default routes advertised by the Multiprotocol Interconnect module when acting as an area border router. To do so, you must select *OSPF Area Default Metric Table* from the *OSPF Menu*. An example of the resulting panel is shown in Figure 172.

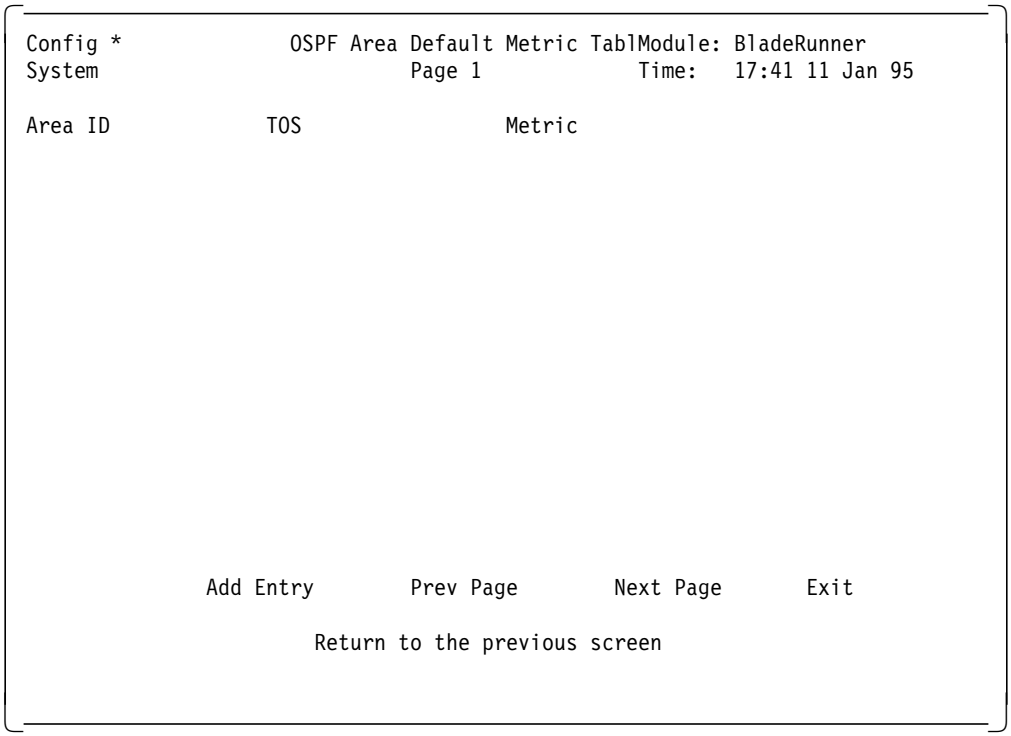


Figure 172. LMS OSPF Area Default Metric Table

This table allows you to specify the following parameters for each entry:

- *Area ID*

  This is the 32-bit integer identifying the Stub Area.

- *TOS*

  This parameter specifies the Type Of Service associated with the metric.

- *Metric*

  This parameter contains the metric value applied at the indicated Type Of Service.

5. You can define a range for an area. Ranges are address/mask pairs that allow you to group subnetted networks that reside in the same area, and to have that group be advertised by *one* network summary advertisement. Otherwise, a summary advertisement would be generated for each subnet in the area. To define a range for an area, select *OSPF Area Address Range*

from the *OSPF Menu*. The resulting panel is shown in Figure 173 on page 295.

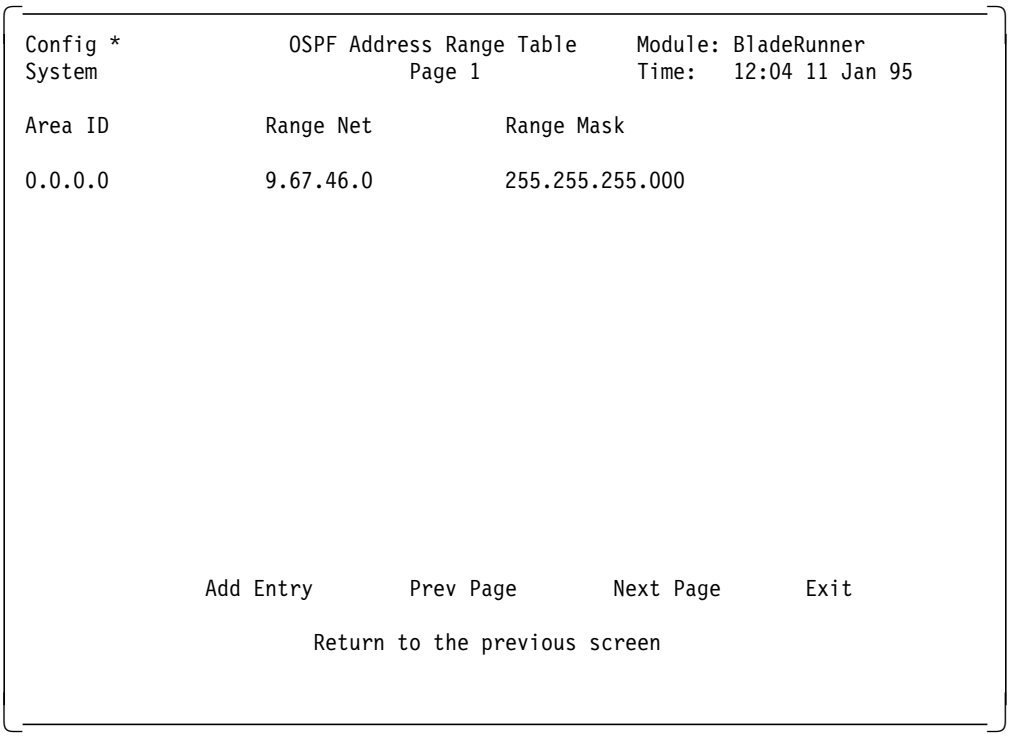


Figure 173. LMS OSPF Area Address Range Panel

The panel allows you to define the following parameters for each entry:

- *Area ID*

  This a 32-bit integer uniquely identifying the area in which the address range is to be found.

- *Range Net*

  This is the IP address of the network or subnetwork indicated by the range. This parameter allows you to assign a single network address to a group of subnets. This network address, together with the subnet mask you provide, specifies the subnets to be grouped in this area range. Just one link summary advertisement will be generated for all subnets in this range, rather than one link summary for each of the subnets included in that network.

- *Range Mask*

  This parameter specifies the subnet mask that pertains to the network or subnetwork specified in the Range Net parameter.

For example, if we specify Range Net 9.67.46.0 and Range Mask 255.255.255.0. It means that the link summary advertisement generated will summarize networks 9.67.46.0 to 9.67.46.254.

Note: When setting up your OSPF network, keep all subnetted networks in the same area.

6. Define the metrics to be advertised for each interface for various Types Of Service (TOS). To do so, select *OSPF Interface Metric Table* from the *OSPF Menu*. An example of the displayed panel is shown in Figure 174 on page 296.

```
Config *              OSPF Interface Metric Table  Module: BladeRunner
System                          Page 1             Time:   17:44 11 Jan 95

IP Address           Port        TOS         Metric

9.67.46.17           0           0           10
9.67.46.44           0           0           10
9.67.46.94           0           0           10

              Add Entry        Prev Page        Next Page       Exit

                      Return to the previous screen
```

Figure 174. LMS OSPF Interface Metric Table

This panel allows you to specify the following parameters for each entry:

- *IP Address*

  This is the IP address of the interface advertising the metric.

- *Port*

  This parameter specifies the port number of this interface.

- *TOS*

  This parameter specifies the Type Of Service metric being referenced.

- *Metric*

  This parameter specifies the metric of using this Type Of Service on this interface.

7. If an area is not directly connected to the backbone area, a virtual link will need to be configured from that area's border router to a border router that connects to the backbone area. This is necessary to restore the continuity of the backbone.

   To define the OSPF virtual links in your OSPF network, select *OSPF Virtual Interface Table* from the *OSPF Menu*. The resulting panel is shown in Figure 175 on page 297.

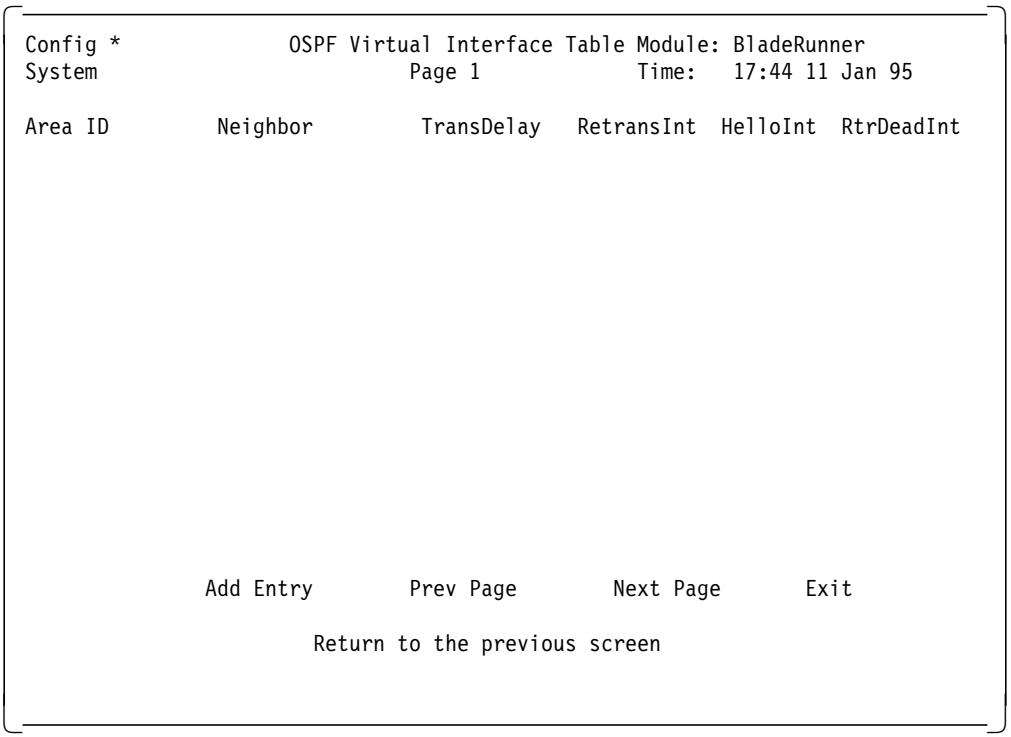


Figure 175. LMS OSPF Virtual Interface Table Panel

The following parameters can be specified for each entry:

- *Area ID*

  This parameter specifies the 32-bit integer identifying the transit area that the virtual link traverses. By definition, this is not 0.0.0.0 (the backbone).

- *Neighbor*

  This parameter specifies the router ID of the virtual neighbor.

- *TransDelay*

  This parameter specifies the number of seconds it takes to transmit a link-state update packet over this interface.

- *RetransiInt*

  This parameter specifies the length of time (in seconds) between link-state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting database descriptions and link-state request packets.

- *HelloInt*

  This parameter specifies the length of time (in seconds) between Hello packets that the router sends on this interface. This parameter must be the same for the virtual neighbor.

- *RtrDeadInt*

  This parameter specifies the length of time (in seconds) that a router's Hello packet will not have been seen before its neighbor declares the router down. This should be some multiple of the Hello interval and must be the same for the virtual neighbor.

8. Define the other OSPF routers which are *neighbors* to the Multiprotocol Interconnect module. To so so, select *OSPF Neighbors* from the *OSPF Menu* panel. An example of the resulting panel is shown in Figure 176 on page 298.

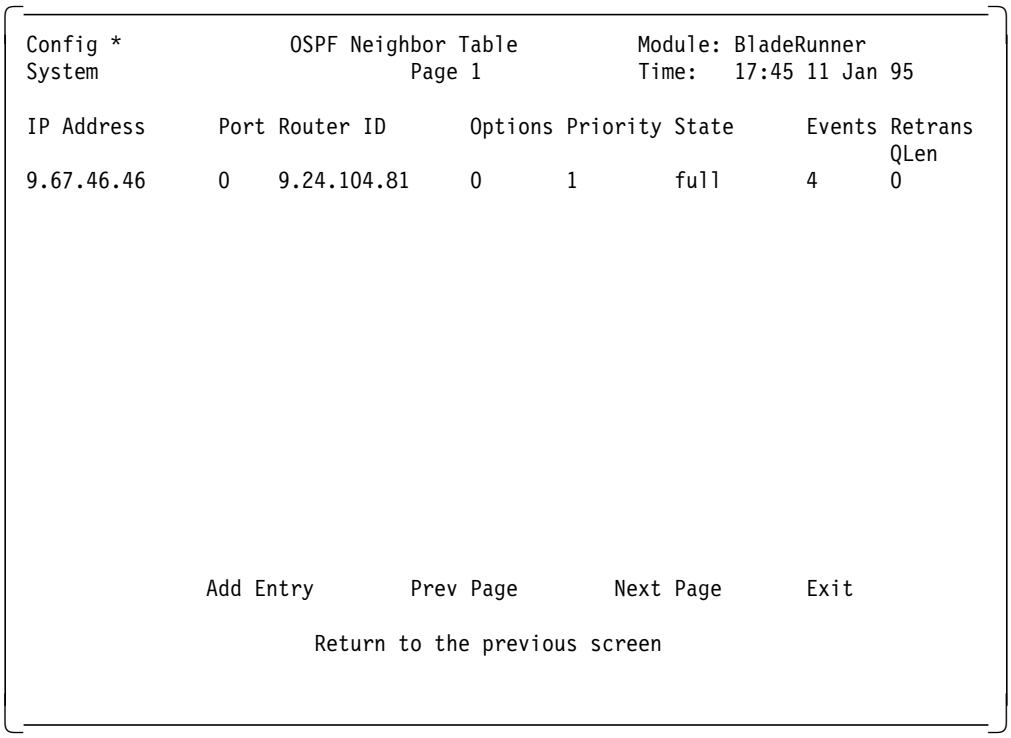


Figure 176. LMS OSPF Neighbors Panel

This panel allows you to describe the following parameters for each neighbor entry:

- *IP Address*

  This parameter specifies the IP address of this neighbor.

- *Port Router ID*

  This parameter specifies the logical port number of this interface. If this interface has been assigned an IP address, this parameter will have a value of 0. If the interface has not been assigned an IP address (a serial WAN port could be an example) the value of this parameter will be equal to the logical port number.

- *Options*

  This field is read-only. It is a bit mask corresponding to the neighbor's options parameter. Bit 0, if set, indicates that the area accepts and operates on external information. If bit 0 is set to zero, it is a Stub Area. Bit 1, if set, indicates that the system will operate on Type Of Service metrics other than 0. If set to zero, the neighbor will ignore all metrics except the TOS 0 metric.

- *Events*

  This parameter is read-only and indicates the number of times this neighbor's relationship has changed state or that an error has occurred.

- *Retrans QLen*

This field is read-only and shows the current length of the retransmission queue.

9. You may define the filters for importing RIP discovered routes by selecting *OSPF RIP Filter Table* from the *OSPF Menu*. An example of the resulting panel is shown Figure 177.

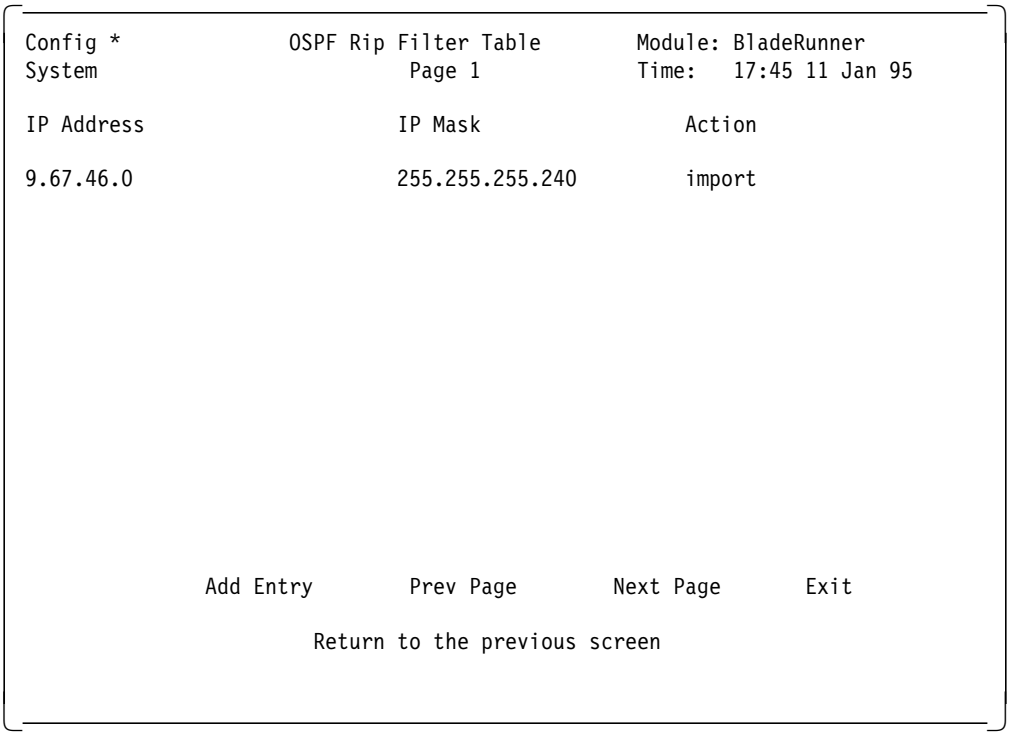


Figure 177. LMS OSPF RIP Filter Table Panel

This panel allows you to enter the following parameters for each filter table entry:

- *IP Address*

  This parameter specifies the destination IP address found by RIP to which this filter should be applied.

- *IP Mask*

  This parameter specifies the mask associated with the IP address.

- *Action*

  This parameter specifies whether to import a route in case of a match.

10. You may define a conversion table that contains information for converting RIP's hop count to OSPF's metric for each configured pair of destination IP address and its mask. To do so, select *RIP Convert Table* from the *OSPF Menu*. An example of the resulting panel is shown in Figure 178 on page 300.

```
Config *              OSPF Rip Convert Table       Module: BladeRunner
System                          Page 1             Time:   17:46 11 Jan 95

IP Address             IP Mask                 Hop Count       Metric

9.67.46.0              255.255.255.240         1               10
9.67.46.0              255.255.255.240         2               20
9.67.46.0              255.255.255.240         3               30
9.67.46.0              255.255.255.240         4               40
9.67.46.0              255.255.255.240         5               50
9.67.46.0              255.255.255.240         6               60
9.67.46.0              255.255.255.240         7               70
9.67.46.0              255.255.255.240         8               80
9.67.46.0              255.255.255.240         9               90
9.67.46.0              255.255.255.240         10              100




              Modify Entry     Prev Page        Next Page       Exit

                       Return to the previous screen
```

Figure 178. LMS Configuration Panel

This panel allows you to enter the following parameters for each entry:

- *IP Address*

  This parameter specifies the destination IP address found by RIP.

- *IP Mask*

  This parameter specifies the destination IP address mask.

- *Hop Count*

  This parameter specifies hop count measured in RIP.

- *Metric*

  This parameter specifies the metric in OSPF converted from RIP.

11. If you have not defined the conversion information for an imported RIP entry, the *RIP Default Conversion Table* will be used. This table is set with a number of default entries when the Multiprotocol Interconnect module is shipped. You can view and/or modify the contents of this table by selecting *OSPF RIP Default Convert Table* from the *OSPF Menu* panel. The resulting display is shown in Figure 179 on page 301.

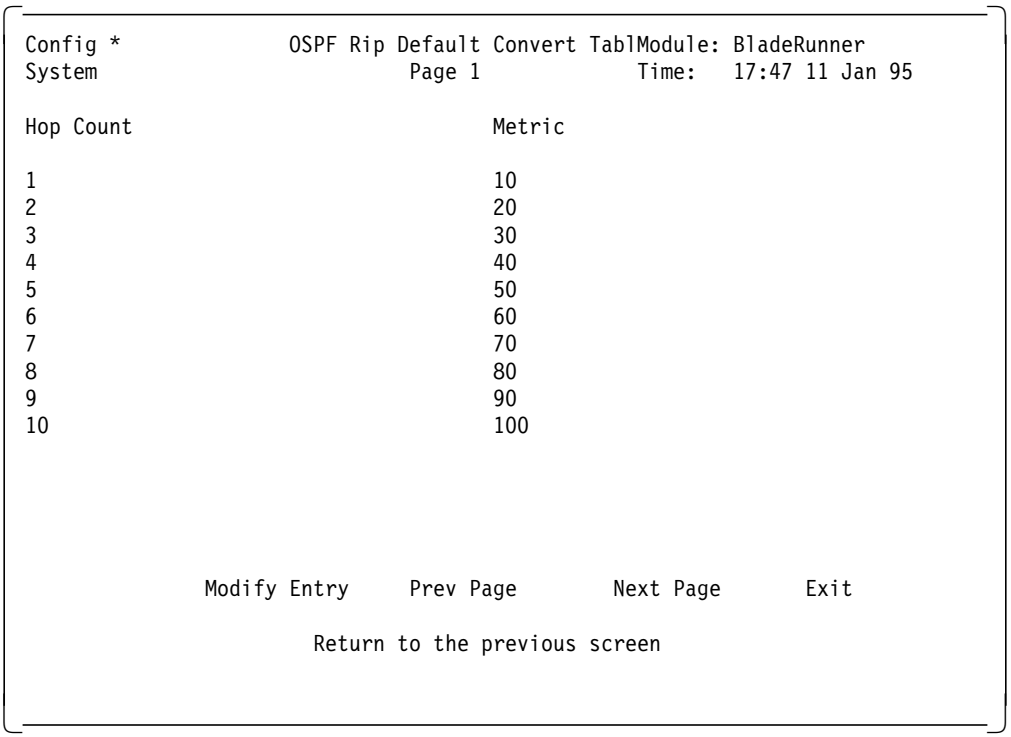


Figure 179. LMS OSPF Default RIP Convert Table Panel

The following parameters can be viewed/modified for each entry:

- *Hop Count*

  This parameter specifies hop count measured in RIP.

- *Metric*

  This parameter specifies the metric in OSPF converted from RIP.

12. You may define a filter for importing static routes by OSPF by selecting *OSPF Static Route Filter Table* from the *OSPF Menu*. An example of the resulting panel is shown in Figure 180 on page 302.

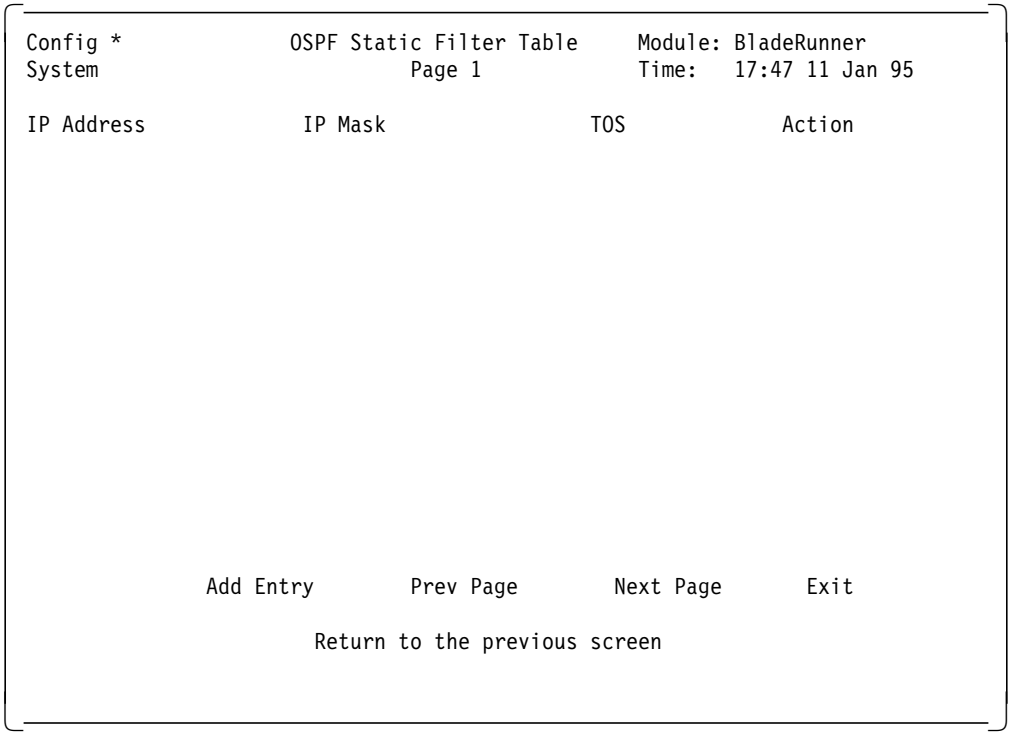


Figure 180. LMS OSPF Static Filter Table Panel

This panel allows you to define the following parameters for each filter entry:

- *IP Address*

  This parameter specifies the destination IP address.

- *IP Mask*

  This parameter specifies the mask associated with the IP address.

- *TOS*

  This parameter specifies the Type Of Service for this route.

- *Action*

  This parameter specifies whether to import a route in case of a match.

13. You may define a conversion table that contains information for converting static route's hop count to an OSPF's metric for each configured pair of destination IP address and its mask. To do so, select *OSPF Static Convert Table* from the *OSPF Menu*. An example of the resulting panel is shown in Figure 181 on page 303.

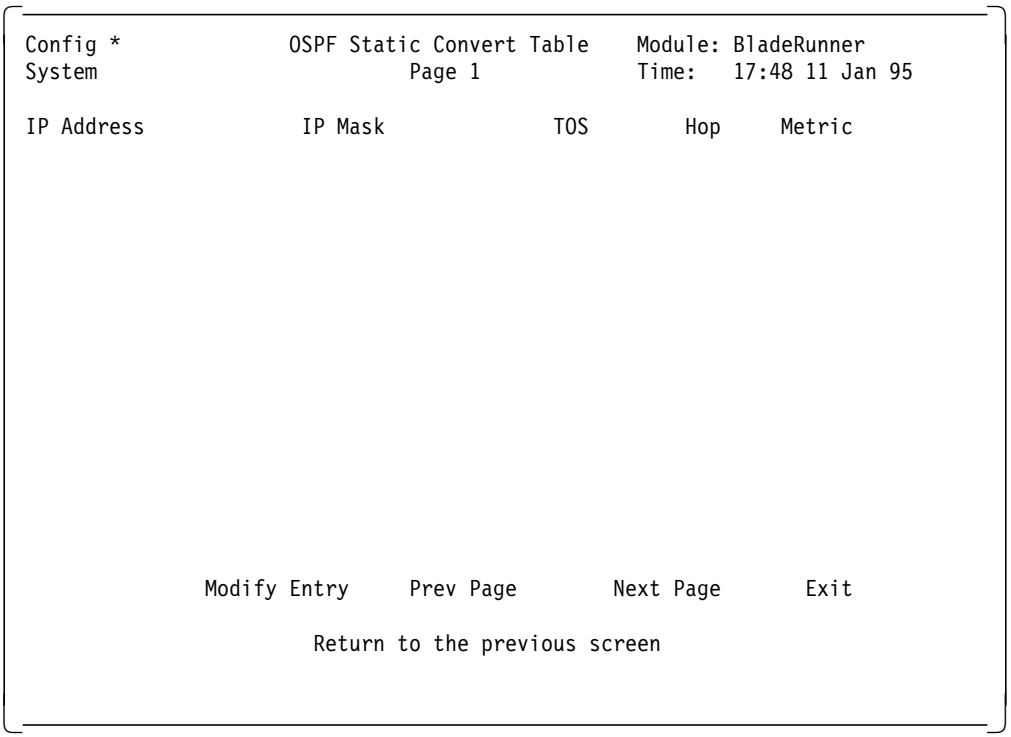


Figure 181. LMS Configuration Panel

This panel allows you to enter the following parameters for each entry:

- *IP Address*

  This parameter specifies the destination IP address.

- *IP Mask*

  This parameter specifies the destination IP address mask.

- *TOS*

  This parameter specifies the Type Of Service for this route.

- *Hop Count*

  This parameter specifies hop count for this static route.

- *Metric*

  This parameter specifies the metric in OSPF converted from static route.

14. If you have not defined the conversion information for an imported static route, the *Static Default Conversion Table* will be used. This table is set with a number of default entries when the Multiprotocol Interconnect module is shipped. You can view and/or modify the contents of this table by selecting *OSPF Static Default Convert Table* from the *OSPF Menu* panel. The resulting display is shown in Figure 182 on page 304.

```
Config *          OSPF Static Default Convert TablModule: BladeRunner
System                          Page 1             Time:   17:49 11 Jan 95

TOS            Hop Count       Metric

0              1               10
0              2               20
0              3               30
0              4               40
0              5               50
0              6               60
0              7               70
0              8               80
0              9               90
0              10              100




               Modify Entry     Prev Page        Next Page       Exit

                        Return to the previous screen
```

Figure 182. LMS OSPF Default Static Convert Table Panel

The following parameters can be viewed/modified for each entry:

- *Hop Count*

  This parameter specifies hop count measured in RIP.

- *Metric*

  This parameter specifies the metric in OSPF converted from RIP.

15. You may define filtering information for IP packets as described in 11.8.9, “IP Security.”

11.8.9 IP Security

IP security feature of the Multiprotocol Interconnect module allows you to define filters which are used to determine which IP packets are forwarded and which ones are discarded when the Multiprotocol Interconnect module is performing IP routing functions.

The IP security feature is comprised of up to 31 different *Security Tables* and a *Security Access List*. Each security table can contain up to 64 address entries and is identified by a *list no*.

To use IP security, you must do the following:

1. Create one or more *IP security tables* to define the filtering information against which the incoming packets may be checked. To do so, you must select *IP Security Table* from the *IP Menu*. An example of an IP security table is shown in Figure 183 on page 305.

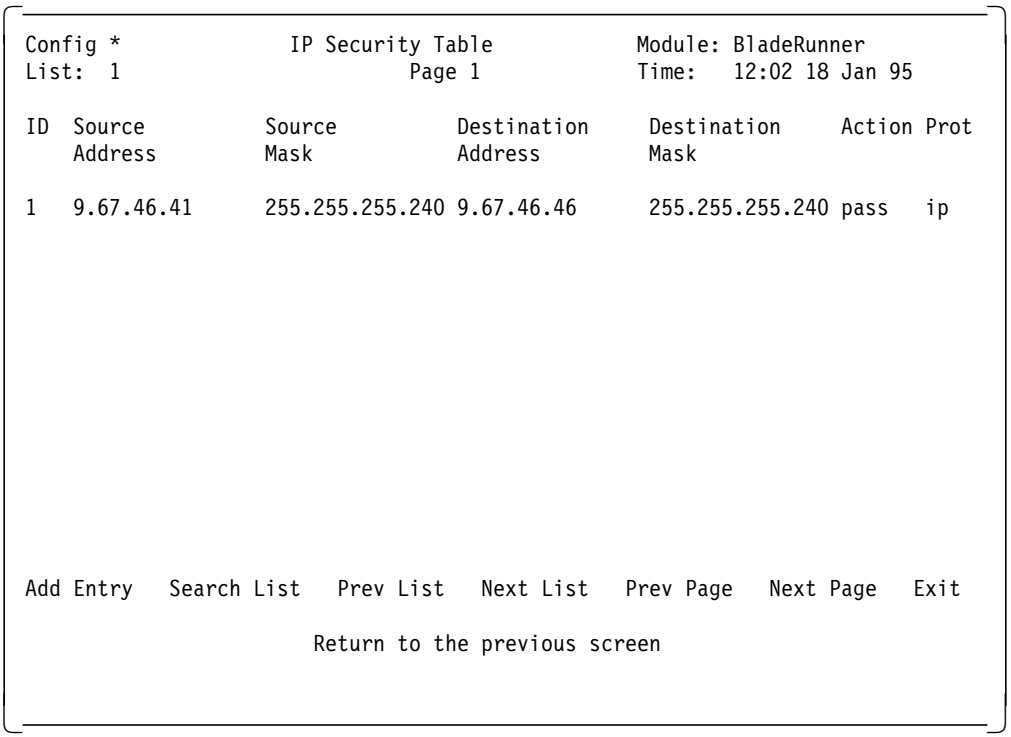


Figure 183. LMS IP Security Table Panel

This table contains the filtering information which specifies the protocol type (IP, ICMP, UDP, or TCP) as well as the source and destination IP addresses/masks against which the incoming and outgoing packets may be checked. This checking is done on the packets received or routed by the Multiprotocol Interconnect module. No checking will be done on the packets generated by the module itself.

To add an entry to this table, select *Add Entry*. A pop-up menu will allow you to specify the following parameters:

- *ID*

  This parameter is a unique numeric identification number for each Security Table entry.

- *Protocol*

  This parameter allows you to select this entry's protocol field. The valid values are IP, ICMP, UDP, or TCP.

- *Action*

  This field indicates the action to be taken on a frame that matches the criteria configured in the source and/or destination address/mask field entries. The valid options are *block* or *pass*.

- *Operator*

  The operator is used to compare the received contents of the received packet against the criteria defined via the source and/or destination address/mask entries. It is also used to compare the contents of the *operand* with the destination TCP/UDP port number stored in the incoming datagram.

  The valid values for the operand are lt (less than), gt (greater than), eq (equal), and neq (not equal).

- *Source Address*

  This is the source address of the IP datagram against which the source address of the IP datagram currently being processed is compared. A value of 0.0.0.0 serves as a wildcard, indicating all IP addresses.

- *Source Mask*

  This is the address mask which is *logically ANDed* with the source address in the table and the source address in the IP datagram. The two results are then compared using the *operator* parameter.

- *Destination Address*

  This is the destination address of the IP datagram against which the destination address of the IP datagram currently being processed is compared. A value of 0.0.0.0 serves as a wildcard, indicating all IP addresses.

- *Destination Mask*: This is the address mask which is *logically ANDed* with the destination address in the table and the destination address in the IP datagram. The two results are then compared using the *operator* parameter.

- *Option*

  This parameter specifies whether an IP datagram with the options set in the frame header should be subjected to the specified tests. This parameter can have a *false* or *true* value. *False* means that the IP datagram with options is not subjected to security tests. This parameter has no affect on IP datagrams with no options.

- *Operand*

  This field specifies the number of the TCP or UDP destination port to be compared with the incoming packet, according to the value configured for *operator*.

Note: When displaying the contents of the IP security table, only a subset of parameters set for each entry are displayed on the screen. To view the remaining parameters, highlight the entry and press the Enter key.

An IP Security table may contain up to 64 entries.

2. Create an *IP Security Access List* to specify whether received or transmitted (or both) packets are to be checked for each IP Security table defined in the previous step. It also defines the action to be taken when a received or transmitted packet matches the criteria defined in the Security table. To define the IP security access list, you must select *IP Security Access List* from the *IP Menu*. An example of the panel which is displayed is shown in Figure 184 on page 307.

```
Config *          IP Security Access List        Module: BladeRunner
                              Page 1             Time:   12:07 18 Jan 95

List    Transmit      Action on       Receive      Action on        ICMP
 No.     Check       No Match (Tx)     Check      No Match (Rx)   Generation
 1       Enabled        pass          Enabled        pass          Enabled
 2       Disabled       pass          Disabled       pass          Disabled
 3       Disabled       pass          Disabled       pass          Disabled
 4       Disabled       pass          Disabled       pass          Disabled
 5       Disabled       pass          Disabled       pass          Disabled
 6       Disabled       pass          Disabled       pass          Disabled
 7       Disabled       pass          Disabled       pass          Disabled
 8       Disabled       pass          Disabled       pass          Disabled
 9       Disabled       pass          Disabled       pass          Disabled
 10      Disabled       pass          Disabled       pass          Disabled
 11      Disabled       pass          Disabled       pass          Disabled
 12      Disabled       pass          Disabled       pass          Disabled



     Modify Entry          Prev Page          Next Page          Exit

                Modify an entry in the IP Security List
```

Figure 184. LMS IP Security Access Panel

This panel allows you to define the following parameters for each entry:

- *List No.*

  This field identifies a security table. It corresponds with the *List No* displayed on the upper left hand corner of the security table.

- *Transmit Check*

  This parameter determines whether IP datagrams to be transmitted on the interface are checked to see if they match the entries in the security table.

- *Action on No Match*

  This parameter specifies whether to allow an IP datagram that does not match the criteria defined in the corresponding Security table to be forwarded to its destination (pass) or to be discarded (block). If two tables are assigned to the same port and the Action on No Match parameters are not the same, the values configured for Security Access List 2 take precedence.

- *Receive Check*

  This parameter determines whether IP datagrams received on the interface are checked to see if they match the entries in the Security table.

- *Action on No Match*

  This parameter specifies whether to allow an IP datagram that does not match the criteria defined in the corresponding security table to be forwarded to its destination (pass) or to be discarded (block). If two tables are assigned to the same port and the Action on No Match parameter are not the same, the values configured for the security access list 2 takes precedence.

- *ICMP Generation*

  This field specifies whether an ICMP Destination Unreachable message is forwarded to the source address on any IP datagram that is discarded because of security checks.

Note: There is only one IP security access list per Multiprotocol Interconnect module.

IP security access list may contain up to 32 entries.

3. Enable IP security on the module, using the *IP System Parameters* panel.
4. Specify up to two IP security lists for each IP port using the *IP Port Parameters* panel.

   Note: A single IP security table may be active on any number of ports at the same time.

11.8.10 Configuring for IPX Routing

The Multiprotocol Interconnect module allows you to configure it as an IPX router. To do so, you must perform the following steps:

1. Configure the system-wide parameters for the Multiprotocol Interconnect module as described in 11.8.1, “Configuring System Wide Parameters” on page 252.
2. Configure the port parameters for the Multiprotocol Interconnect module’s ports as described in 11.8.2, “Configuring Port Parameters” on page 255.
3. Select *IPX* from the *Protocols Menu*. A panel as shown in Figure 185 will be displayed.

```
Config *                          IPX Menu        Module: BladeRunner
                                                  Time:   10:49 13 Jan 95



                                IPX System Parameters

                                IPX Port Parameters

                                IPX Routing Table

                                IPX SAP Bindery Table

                                IPX Security Access List

                                IPX Security Table

                                Exit



                        Enter the IPX system parameters screen
```

Figure 185. LMS IPX Menu Panel

This panel allows you to access all the panels for viewing and configuring the IPX parameters supported by the Multiprotocol Interconnect module.

4. Configure the system-wide IPX parameters by selecting *IPX System Parameters* from the *IPX Menu*. An example of the resulting panel is shown in Figure 186 on page 309.

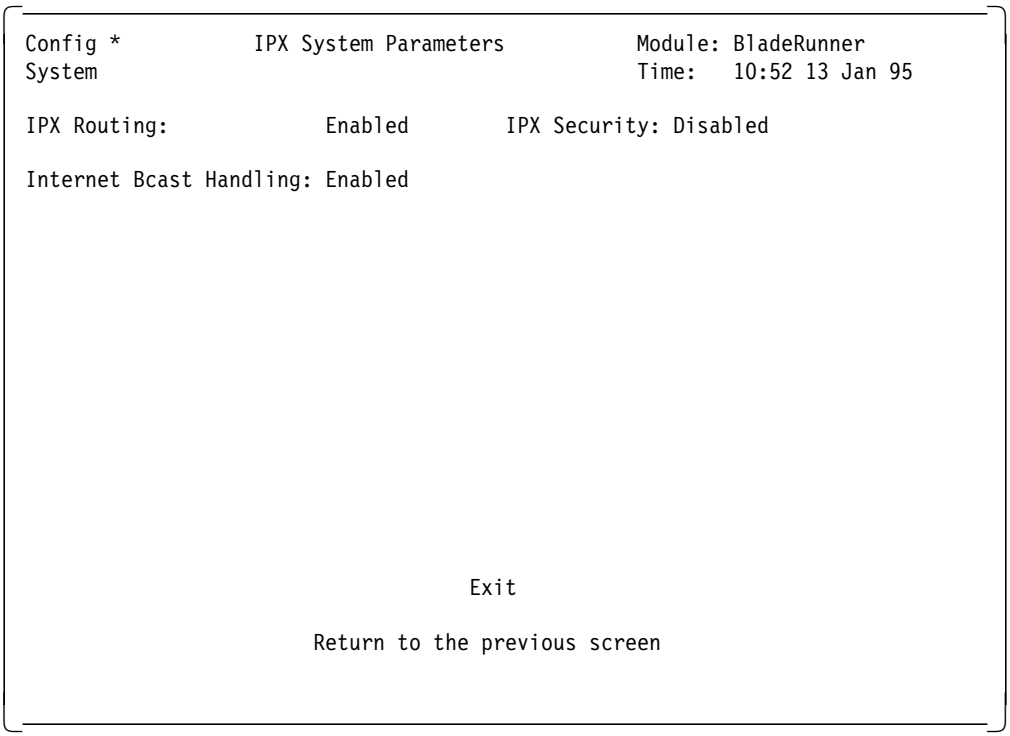


Figure 186. LMS IPX System Parameters Panel

This panel allows you to view and modify the following system-wide IPX parameters for the Multiprotocol Interconnect module:

- *IPX Routing*

  This parameter allows you to enable IPX routing at the module level. Note that you must also enable IPX routing at each port which is to participate in IPX routing.

- *IPX Security*

  This parameter enables/disables IPX security features of the Multiprotocol Interconnect module. The IPX security is similar to the IP security discussed in 11.8.9, “IP Security” on page 304.

- *Internet Bcast Handling*

  This parameter specifies if the broadcast packets are forwarded or discarded by the Multiprotocol Interconnect module.

5. Configure IPX routing for each port that is to perform IPX routing. To do so, you must select *IPX Port Parameters* from the *IPX Menu* panel. An example of the IPX Port Parameters panel is shown in Figure 187 on page 310.

```
Config *            IPX Port Parameters            Module: BladeRunner
Log. Port: 1   LOGICAL PORT                        Time:   11:00 13 Jan 95

IPX Port Routing:       Enabled         Host Number:            08008F4001A0

Disposition:            discard         Network Number:         00000001

Interface Delay:        1               Encapsulation:          ieee802.3

RIP Timer:              30              SAP Timer:              60

Security Access List 1: 0               Security Access List 2: 0









        Search Port         Prev Port         Next Port         Exit

                      Return to the previous screen
```

Figure 187. LMS IPX Port Parameters Panel

This panel allows you to configure the following IPX parameters for each port:

- *IPX Port Routing*

  This parameter allows you to enable IPX routing for this port. Note that the IPX routing must be enabled at the module level for this port to be able to route IPX packets.

- *Host Number*

  This parameter is read-only and displays the host address of the selected port.

  On LAN ports that support IEEE 802.3 addressing, the host number is the IEEE 802.3 MAC address of the physical port.

  On WAN ports and LAN ports that do not support IEEE 802.3 addressing, the port takes the lowest IEEE 802.3 MAC address in the Multiprotocol Interconnect module.

- *Disposition*

  This parameter specifies if the IPX traffic received by this port is to be bridged or discarded. This parameter is only valid when IPX routing is enabled at the module level but is disabled for this port.

- *Network Number*

  Each port that supports IPX routing must be assigned an IPX address before the IPX routing can become active on that port.

  The IPX address consists of the network number and the host number. The network number is a 32-bit hexadecimal number that identifies the network to which this port is attached.

  Note: Each port must have a different network number assigned to it.

- *Interface Delay*

  This is the estimated time taken for an IPX packet containing 576 bytes of data to traverse the hop between the interface and the associated link. This parameter is displayed in milliseconds and is used to determine the best route to a destination address.

  If there are more than one route with different interface delay, the one with the lowest value will be the best route. If the interface delay between two or more routes is the same, the one advertised first will be selected.

- *Encapsulation*

  This parameter specifies the LAN encapsulation used when IPX datagrams are transmitted on this interface. The four options are:

  – Ethernet

  – IEEE 802.2

  – SNAP

  – IEEE 802.3

  The IPX routing element accepts IPX datagrams encapsulated by any of these four formats.

- *Security List n*

  This parameter specifies the number identifying the IPX Security Access list associated with this port. You may attach two access lists to each port. Note that the IPX Security parameter must be set to enabled before these lists can be used. A value of 0 for this parameter indicates that this list is inactive.

6. You may use IPX security to set the filtering criteria for the Multiprotocol Interconnect module when performing IPX routing functions.

   The IPX security feature is comprised of up to 31 different Security tables and a security access list. Each security table may contain up to 64 entries.

   The operation of the IPX security is the same as the IP security which is discussed in 11.8.9, “IP Security” on page 304.

11.9 Monitoring Multiprotocol Interconnect Module

The *Status Menu* allows you to view the statistical information provided by the Multiprotocol Interconnect module.

The following is a summary description of the options which are available via the Status Menu:

- *Station Statistics*

  Displays information about Interconnect module and the software installed on it.

- *Buffer Pool Table*

  Shows the number of buffers and the amount of heap memory in use on the Multiprotocol Interconnect module.

- *Physical Port List*

Allows you to display information about the physical ports currently installed on your module.

- *Physical Port Protocol Statistics*

  Displays different statistical information for each port, depending on the type of the interface and the link protocol configured for the port.

- *Physical Interface Statistics*

  This screen is applicable to the WAN ports only.

- *Logical Port Statistics Screen*

  Displays statistical information about the packets sent and received on a logical port.

- *Logical Port Multilink Statistics*

  This screen is applicable to the WAN ports only.

- *Transparent Bridging System Statistics*

  Provides statistical information about the frames sent and received by the Multiprotocol Interconnect module using transparent bridging.

- *Transparent Bridging Port Statistics*

  Provides statistical information about the frames sent and received on each port by the Multiprotocol Interconnect module using transparent bridging.

- *Source Routing Port Statistics*

  Provides statistical information about the frames sent and received on each port by the Multiprotocol Interconnect module using source-route transparent bridging.

- *STP System Statistics*

  Displays system-wide spanning tree protocol statistics.

- *STP Port Statistics Screen*

  Displays the spanning tree statistics for each port.

- *IP System Statistics*

  Displays statistical information about the IP packets sent and received by the Multiprotocol Interconnect module.

- *IP Port Statistics*

  Displays statistical information about the IP packets sent and received by the Multiprotocol Interconnect module.

- *ICMP System Statistics*

  Displays statistical information about the ICMP packets sent and received by the Multiprotocol Interconnect module.

- *ICMP Port Statistics*

  Displays statistical information about the ICMP packets sent and received on each port by the Multiprotocol Interconnect module.

- *ICMP Timers*

  Displays the date and time of the various categories of ICMP messages that were sent and received by the Multiprotocol Interconnect module.

- *OSPF System Statistics*

Displays information about various link state advertisements sent and received by the Multiprotocol Interconnect module.

- *OSPF Link State Database Table*

  Displays the link state database in the Multiprotocol Interconnect module. This information includes the area and the router identifier from which the link-state advertisements were received.

- *OSPF Virtual Neighbor Table*

  Displays all the virtual neighbors.

- *UDP System Statistics*

  Displays statistical information about UDP datagrams sent and received by the Multiprotocol Interconnect module.

- *DECnet IV System Statistics*

  Displays statistical information about the DECnet IV packets sent and received by the Multiprotocol Interconnect module.

- *DECnet IV Port Statistics*

  Displays statistical information about the DECnet IV packets sent and received on each port by the Multiprotocol Interconnect module.

- *IPX System Statistics*

  Displays statistical information about the IPX packets sent and received by the Multiprotocol Interconnect module.

- *IPX Port Statistics*

  Displays statistical information about the IPX packets sent and received on each port by the Multiprotocol Interconnect module.

- *Significant Events*

  This screen provides you with information about the events on the Multiprotocol Interconnect module.

Appendix A. Power Requirements for 8250/8260 Modules

A.1 Power Requirements for 8250 Ethernet Modules

Table 41. Power Requirements for 8250 Ethernet Modules

Module	Feature Code	Type	Description	# of Slots Used	Power Consumption (watts by voltage type)				
					+5	+12	-12	-5	-2
10BASE-T	3800E	Ethernet	8 ports 8-pin UTP STP	One	10	0	0	0	0
10BASE-T	3801E	Ethernet	12 ports TELCO UTP	One	11	0	0	0	0
10BASE-T	3829E	Ethernet Ethernet	24 ports Port switch TELCO UTP	One	9	0	0	0	0
Security	7385	Ethernet	12 ports Security TELCO	One	11	0	0	0	0
Transceiver	3803ET	Ethernet	3 ports AUI male	One	9	0	0	0	0
Repeater	3804ER	Ethernet	2 ports AUI female	One	6	0	0	0	0
Fiber	3805EF-07EF	Ethernet	4 ports	One	8	0	0	0	0
Fiber	3808EF-10EF 6774, 7391, 7394	Ethernet	4 ports Port switch	One	10	0	0	0	0
Fiber	6775, 7392, 7395	Ethernet	4 ports	One	8	0	0	0	0
Fiber	3811EF-13EF 6773, 7390 7393	Ethernet	2 ports Port switch	One	8	0	0	0	0
FOIRL	3814EFL-16EFL	Ethernet	4 ports	One	10	0	0	0	0
BNC	3817EF	Ethernet	6 ports BNC	One	12	4.5	0	0	0
TCP/IP/LAT terminal server	3818ES, 3896ES	Ethernet	16 ports	One	14	3.5	0	0	0
EMM	3819 3788	Ethernet	Ethernet Mgmt. Module	One	14	0.5	.25	0	0

A.2 Power Requirements for 8250 Token-Ring Modules

Table 42. Power Requirements for 8250 Token-Ring Modules

Module	Feature Code	Type	Description	# of Slots Used	Power Consumption (watts by voltage type)				
					+5	+12	-12	-5	-2
MAU	3820T	Token Ring	8 ports 8-pin RI/RO	One	7	0	0	0	0
Twisted Pair Media	3821T	Token Ring	20 ports 8-pin	Two	12	0	0	0	0
Fiber Repeater	3822TR	Token Ring	ST connec. 8-pin RI/RO	One	11	0	0	0	0
TRMM Basic	3823	Token Ring	Mgmt. Module equipped to provide basic function	One	17	0.5	0.5	0	0
TRMM Advanced	3884	Token Ring	Mgmt. Module equipped to provide advanced function	One	17	0.5	0.5	0	0

A.3 Power Requirements for 8250 FDDI Modules

Table 43. Power Requirements for 8250 FDDI Modules

Module	Feature Code	Type	Description	# of Slots Used	Power Consumption (watts by voltage type)				
					+5	+12	-12	-5	-2
Fiber	3825EF 7388	FDDI	8 ports ST connec. MIC connec.	Two	36	7.5	0	0	0
Shielded Twisted Pair	3826F	FDDI	8 ports DB-9 connec.	Two	36	7.5	0	0	0
FMM	3827	FDDI	Mgmt. Module A/B ports	Two	22	5.5	0	0	0

A.4 Power Requirements for 8250 Internetworking Modules

Table 44. Power Requirements for 8250 FDDI Modules

Module	Feature Code	Type	Description	# of Slots Used	Power Consumption (watts by voltage type)				
					+5	+12	-12	-5	-2
Ethernet Bridge	3828EB	Ethernet	2 ports	Two	20	7.5	.25	0	0
Token Ring Bridge	3883TB	Token Ring	2 ports SR bridge	One	14	0	0	0	0
Token Ring Bridge	3958	Token Ring	2 ports SR/SRT bridge	One	14	0	0	0	0
Ethernet Intercon.	6768 6767	Ethernet	6 ports	Two	31	12	0	0	0

Index

Numerics

A

B

C

D

E

F

I

J

L

M

N

O

P

R

S

T

V

ITSO Technical Bulletin Evaluation RED000

International Technical Support Organization
8260 Multiprotocol Intelligent Switching Hub
May 1995

Publication No. GG24-4370-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:

Do you provide billable services for 20% or more of your time? Yes____ No____

Are you in a Services Organization? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the Bulletin published in time for your needs? Yes____ No____

d) Did this Bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

Name	Address
Company or Organization	
Phone No.	

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department 545, Building 657
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.