IBM 8250 Intelligent Hub and IBM Hub Management Program/6000

Document Number GG24-4033-00

June 1993

International Technical Support Center
Raleigh

Take Note!

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

First Edition (June 1993)

This edition applies to Version 1.0 of the IBM AIX NetView Hub Management Program/6000 (Product Number 5696-364) and the IBM 8250 Multiprotocol Intelligent 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 ITSC 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 Center
Dept. 985, 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.

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

Abstract

This document provides comprehensive information about the installation and configuration of the IBM 8250 Multiprotocol Intelligent Hub and all its modules. It also provides detailed information about how to manage networks based on the IBM 8250 Multiprotocol Intelligent Hub, using the in-band and out-of-band management functions provided by the IBM 8250 management modules and the the IBM AIX NetView Hub Management Program/6000.

To provide the users with the necessary background information, introductions to Ethernet, FDDI, LAN Bridging standards, and TCP/IP have also been included in this document.

This document was written for network managers, network architects and system engineers who need to implement token-ring, Ethernet and/or FDDI networks which incorporate the IBM 8250 Multiprotocol Intelligent Hub and the AIX Netview Hub Management Program/6000. Some knowledge of networking architectures and protocols is assumed.

CO (380 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 8250 Multiprotocol Intelligent Hub and IBM AIX NetView Hub Management Program/6000. The information in this publication is not intended as the specification of any programming interfaces that are provided by the above products. See the PUBLICATIONS section of the IBM Programming Announcement for each of the above products 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 Commercial Relations, IBM Corporation, Purchase, NY 10577.

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.

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, which are denoted by an asterisk (*) in this publication, are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
InfoExplorer
PS/2
AIX/6000
NetView
RISC System/6000
IBM
OS/2

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

DEC VT52, DEC VT100, DEC VT220, LAT and DECnet	Digital Equipment Corporation
Chipcom and ONline	Chipcom Corporation
Unix	AT&T
Ethernet	Xerox Corporation
Intel	Intel Corporation
Microsoft	Microsoft Corporation
Novell, IPX and Netware	Novell, Inc.
3Com	3Com Corporation

Preface

This document will assist customers and systems engineers to implement local area networks based on the IBM 8250 Multiprotocol Intelligent Hub and managed by the IBM AIX NetView Hub Management Program/6000.

The document is organized as follows:

- Part 1, “Concepts and Architectures”

  This section provides information on local area networking concepts and communication protocols.

  - Chapter 1, “Local Area Networks and Intelligent Hubs”

    This chapter introduces intelligent hubs.

  - Chapter 2, “Ethernet,Token-Ring and FDDI Overview”

    This chapter introduces Ethernet, token-ring and FDDI standards and describes the various physical components that are used in local area networks using these standards.

  - Chapter 3, “Bridging Standards”

    This chapter explains various types of bridging standards (transparent, source routing and source routing transparent) used in local area networks today.

  - Chapter 4, “ TCP/IP Overview”

    This chapter overviews the TCP/IP protocol suite.

  - Chapter 5, “ AIX NetView/6000 Overview”

    This chapter describes the IBM AIX NetView/6000 product.

- Part 2, “8250 Description, Installation, Configuration”

  This section describes the IBM 8250, its installation and the configuration of its various modules.

  - Chapter 6, “ IBM 8250 Multiprotocol Intelligent Hub Overview”

    This chapter provides an overview of the functions and facilities offered by the IBM 8250 Multiprotocol Intelligent Hub.

  - Chapter 7, “8250 Ethernet Modules and Accessories”

    This chapter provides descriptions and installation information about the 8250 Ethernet modules.

  - Chapter 8, “Ethernet Terminal Server Module”

    This chapter provides descriptions and installation information about the 8250 Ethernet Terminal Server module.

  - Chapter 9, “Ethernet Design Considerations”

    This chapter describes design considerations using the 8250 Ethernet modules.

  - Chapter 10, “8250 Token-Ring Modules and Accessories”

    This chapter provides descriptions and installation information about the 8250 token-ring modules.

- Chapter 11, “8250 FDDI Modules”

  This chapter provides descriptions and installation information about the 8250 FDDI modules.

- Part 3, “8250 Management”

  This section describes the management functions provided by the IBM 8250 management modules and the AIX NetView Hub Management Program/6000.

  - Chapter 12, “ Hub Management - Before You Start”

    This chapter describes the tasks that should be performed before using the 8250 management products.

  - Chapter 13, “AIX NetView Hub Management Program/6000”

    This chapter describes the AIX Hub Management Program/6000.

  - Chapter 14, “Ethernet Management Functions”

    This chapter provides information about managing 8250 Ethernet Local Area Networks.

  - Chapter 15, “Token-Ring Management Functions”

    This chapter provides information about managing 8250 token-ring local area networks.

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 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide*, GA33-0191
- *IBM Cabling System Planning and Installation Guide*, GA27-3361
- *IBM Token-Ring Network Introduction and Planning Guide*, GA27-3677
- *IBM Cabling System Optical Fiber Planning and Installation Guide*, GA27-3943
- *IBM FDDI Introduction and Planning Guide*, GA27-3892

Related manuals packaged with the product:

- *8250-006 Installation Guide*, SA33-0192
- *8250-017 Installation Guide*, SA33-0195
- *8250-6HC Installation Guide*, SA33-0235
- *Fault-Tolerant Controller Installation Guide*, SA33-0193

IBM 8250 Ethernet Modules:

- *Ethernet 10BASE-T Module Installation Guide*, SA33-0196
- *Ethernet 50-Pin Module Installation Guide*, SA33-0197
- *Ethernet 24-Port 10BASE-T Module Installation Guide*, SA33-0198
- *Ethernet Transceiver Module Installation Guide*, SA33-0199
- *Ethernet Repeater Module Installation Guide*, SA33-0200
- *Ethernet Fiber Module Installation Guide*, SA33-0201
- *Ethernet Port-Switching Fiber Module Installation Guide*, SA33-0202

- *Ethernet FOIRL Module Installation Guide*, SA33-0204
- *Ethernet BNC Module Installation Guide*, SA33-0205
- *Ethernet Terminal Server Reference Guide*, SA33-0206
- *Ethernet Terminal Server Module Installation Guide*, SA33-0207
- *Ethernet Management Module Installation Guide*, SA33-0209
- *Ethernet Bridge Module Installation Guide*, SA33-0218

IBM 8250 Token-Ring Modules:

- *Token-Ring MAU Module Installation Guide*, SA33-0210
- *Token-Ring Media Module Installation Guide*, SA33-0211
- *Token-Ring Fiber Repeater Module Installation Guide*, SA33-0212
- *Token-Ring Network Management Module Installation and Operation Guide*, SA33-0213
- *Token-Ring Network Bridge Module Installation and Operation Guide*, SA33-0219

IBM 8250 FDDI Modules:

- *FDDI Fiber Module Installation Guide*, SA33-0215
- *FDDI STP Module Installation Guide*, SA33-0216
- *FDDI Management Module Installation and Operation Guide*, SA33-0217

IBM AIX NetView/6000:

- *IBM AIX NetView Hub Management Program/6000 User′s Guide*, SH11-3061

International Technical Support Center Publications

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

> *Bibliography of International Technical Support Centers Technical Bulletins*, GG24-3070.

Acknowledgments

The advisor for this project was:

Mohammad Shabani
International Technical Support Center, Raleigh

The authors of this document are:

Wolfgang Binder
IBM Germany

John O′Neill
IBM UK

Alan Smith
IBM Australia

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

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

Ray Collins
International Technical Support Center, Raleigh

Shawn Walsh
International Technical Support Center, Raleigh

Part 1. Concepts and Architectures

Chapter 1. Local Area Networks and Intelligent Hubs

Ethernet local area networks were the first important LANs on the market. In the early 1980s, an Ethernet LAN consisted of a thick yellow bus cable, which formed the network backbone. A workstation could be connected to the bus every 2.5 m. This was a cumbersome task which consisted of drilling the bus cable and mounting a transceiver box on it. The connection between the workstation and the transceiver was made with an Attachment Unit Interface (AUI) cable. The AUI cable could be a maximum of 50 meters in length. See Figure 1 for an example of a thick wire Ethernet.

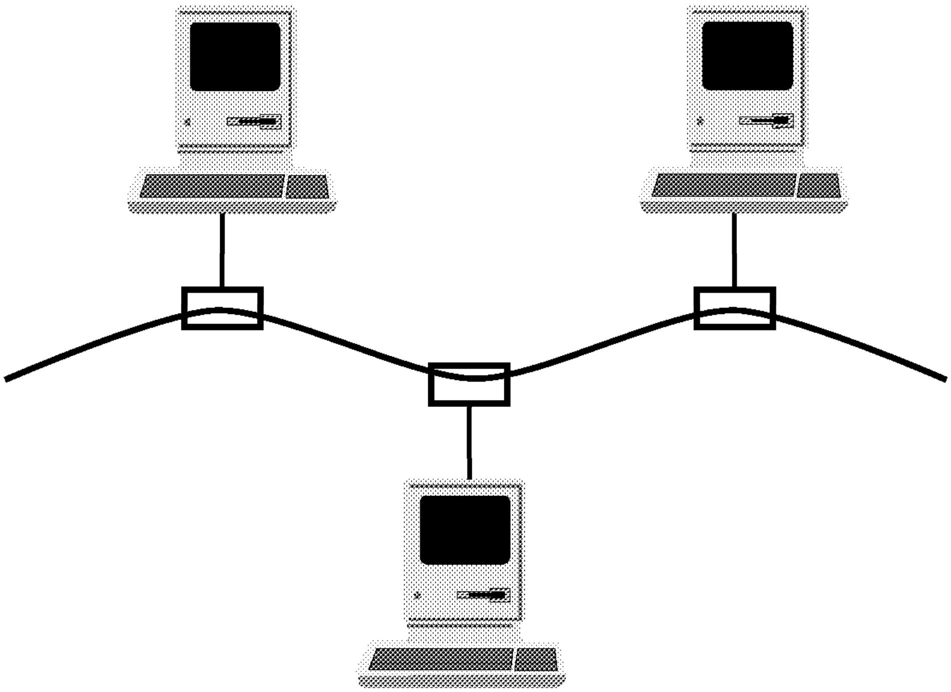


Figure 1. Ethernet in 1980

For their time, these early Ethernet LANs were a good solution for small workgroups. However, these LANs offered very little management facilities due to the bus wiring design. Cable faults were difficult to locate and changes to the network were time consuming.

In the mid 80s, IBM* introduced a structured cabling system with twisted pair cabling and announced the IBM Token-Ring Local Area Network. A token-ring network logically behaves like a ring, but is physically wired in a star configuration, using mostly shielded twisted pair (STP), or more recently, also unshielded twisted pair (UTP) cabling. Figure 2 on page 4 shows a token-ring network consisting of a Multistation Access Unit (MAU) as the concentrator and the lobe cabling running from the concentrator to the workstations.

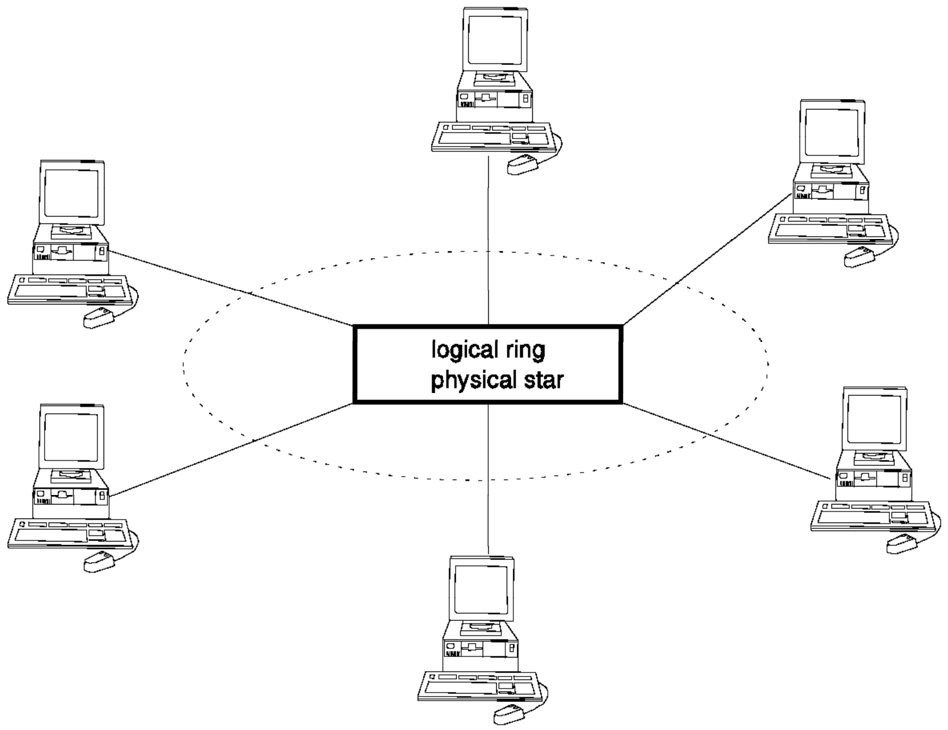


Figure 2. Token-Ring Network

The token-ring architecture also incorporated ring management facilities which are provided via Media Access Control (MAC) frames for error diagnosis and recovery. In a token-ring network, cable faults are detected and can be bypassed automatically. Network management can be done locally on the ring or via a centralized management center. Also, because of the structured wiring, moves and changes are easy to accommodate.

Since token-ring networks are not based on a contention algorithm (as is the case of Ethernet), much more efficient utilization of the available bandwidth is possible in large networks.

The Ethernet community soon adopted the structured wiring using twisted pair cabling and the star configuration using concentrators. This was made possible by the 10BASE-T standard.

Similar to a token-ring network, the Ethernet networks based on the 10BASE-T standard provide flexible network configurations allowing easy reconfiguration of the network for accommodating user relocations and bypassing of faulty cables. Figure 3 on page 5 shows an Ethernet network using a 10BASE-T based *hub*.

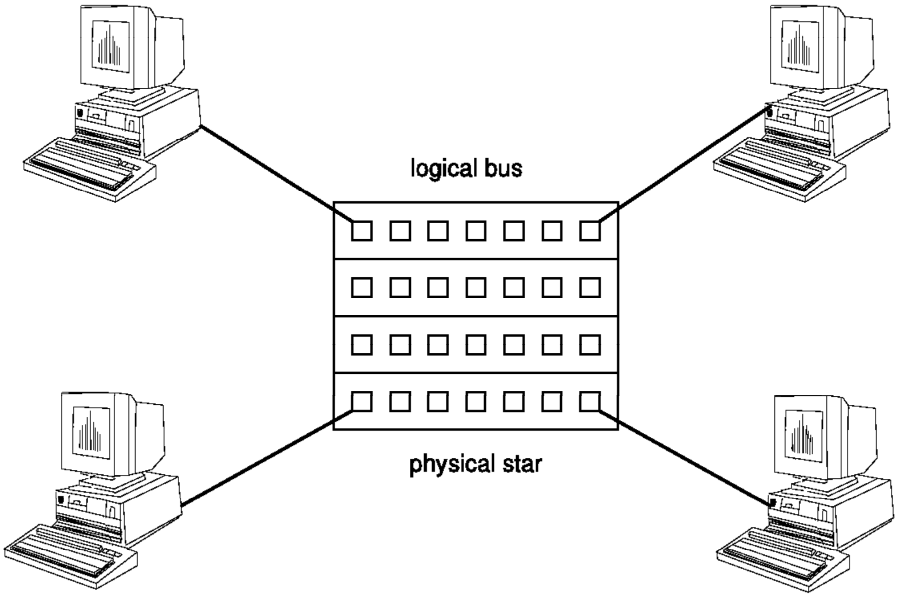


Figure 3. Ethernet 10BASE-T Hub

The first star wired concentrators for Ethernet did not contain much in the way of error recovery or diagnosis capabilities.

The next step in the evolution of wiring concentrators has resulted in the introduction of the so-called *intelligent hubs*. As shown in Figure 4 on page 6, they exist with both, single or multiprotocol capabilities.

The single protocol intelligent hubs are optimized for a single LAN standard. They allow modular growth and LAN segments are linked by external bridges or routers. Management can be done locally or can be integrated into a central management system. The process of installing, configuring and managing single protocol hubs is less complex than it is for multiprotocol hubs.

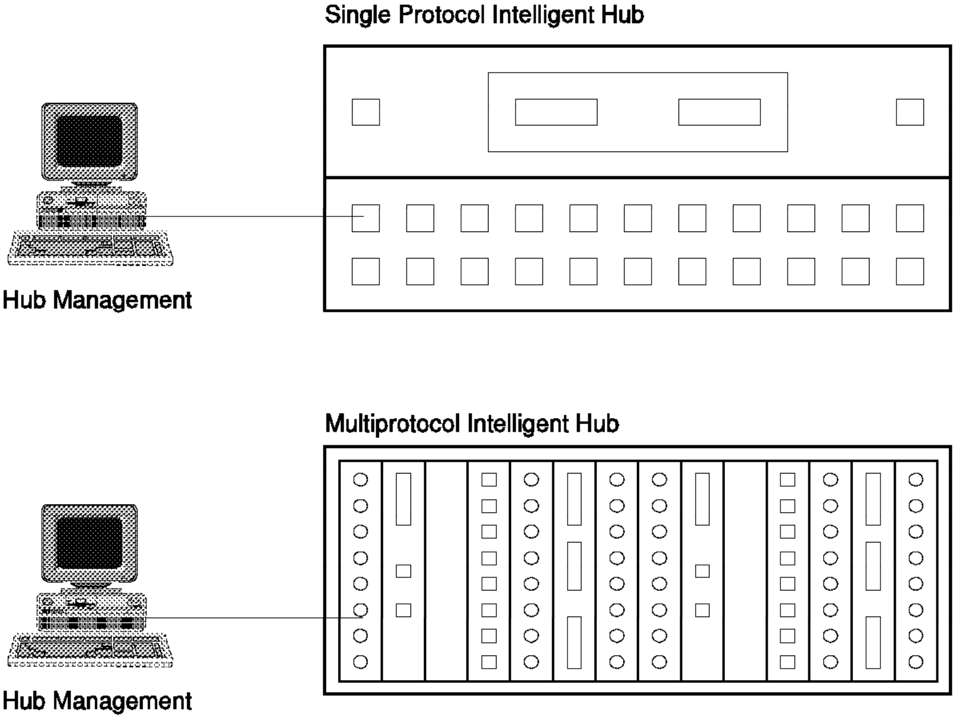

Single Protocol Intelligent Hub
Hub Management
Multiprotocol Intelligent Hub
Hub Management

Figure 4. Single and Multiprotocol Intelligent Hub

The multiprotocol intelligent hub is an integrated solution for a wiring concentrator supporting different types of local area networks using different types of cabling. Normally it integrates Ethernet, token-ring and FDDI support in a single device. Its design is modular, so an upgrade simply means the addition of a card. The hub also has the potential for the integration of bridge and router modules. There is one management interface to a multiprotocol network. Typically, ports are more expensive and the LAN environment is more complex compared to the single protocol hub. An example of a multiprotocol intelligent hub is the IBM 8250 which supports the following functions and features:

- Single or multiple LAN protocols
- Local/remote management
- Network access security
- Automatic network recovery in case of faulty nodes or broken segments
- Network monitoring
- Multiple cable media support (STP, UTP, fiber)
- Port, bank and module switching

  Port switching means that the ports on one module can be assigned to different LANs of the same type. Bank switching is the ability to assign *bank*s of ports to different LANs. Module switching is the ability to attach different modules on the hub to different LANs.
- Redundant components such as controller module, power supply and management module
- Dial-up access to the hub

- Integrated bridge modules

Another distinction for modern hubs is the classification into three different categories:

- Workgroup hub

  A single protocol intelligent hub for the connection of 40 to 60 workstations.

- Midrange hub

  A multiprotocol intelligent hub for a larger number of workstations.

- Super hub

  Also multiprotocol, but with a higher amount of available bandwidth through the use of the ATM (Asynchronous Transfer Mode) transmission method. We foresee that hubs implementing this technology will appear from various manufacturers in the near future.

The IBM 8250 is IBM′s first multiprotocol intelligent hub with a strategic mission to address the needs of customers during 1990s. This document describes the IBM 8250 Multiprotocol Intelligent Hub and provides you with detailed information about design, installation, and management of local area networks using this product.

Chapter 2. Ethernet,Token-Ring and FDDI Overview

This chapter provides background information about IEEE 802.3/Ethernet**, token-ring and FDDI local area networks. It is intended to provide the readers with a brief introduction to the various protocols and topologies used in designing today′s local area networks.

2.1 Ethernet/802.3

Ethernet (802.3) is currently the most widely used LAN protocol in the world. Since its introduction to the marketplace in the seventies it has been established among a wide range of users.

Invented by Xerox** in the early seventies and brought to the marketplace as Ethernet V.1, the protocol was then developed by a consortium of DEC**, Intel** and Xerox. This consortium brought out a new version of Ethernet in 1980 called Ethernet (DIX) V2. They also published the architecture and took it to the Institute of Electrical and Electronics Engineers (IEEE) to have it accepted as an international standard. The IEEE ratified the Ethernet DIX V2 standards with some slight modifications as IEEE 802.3. The 802.3 standard has since been approved by a number of other organizations including the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO 8802-3).

Today both Ethernet and 802.3 LANs are widely implemented across all areas of the marketplace. It has not, as was widely predicted, been replaced by token-ring.

This is largely due to the fact that although the protocol used by Ethernet/802.3 LANs has not changed, the physical topology over which they can be implemented has changed significantly. This has enabled users to have access to some of the benefits (such as manageability) offered by other topologies such as token-ring while still enjoying the perceived advantages of Ethernet/802.3, which include:

1. Wide choice of equipment
2. Low cost of equipment

Though Ethernet 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 chapter applies equally to both Ethernet and 802.3 LANS, the term Ethernet (802.3) will be used throughout this chapter. However, where there are differences, they will be indicated by using the appropriate terminology.

Note

Both Ethernet and the 802.3 protocol can be used on the same physical network simultaneously. However, stations using one protocol cannot interoperate with stations using the other protocol. This is due to the differences which will be explained later in this chapter.

Please note that this document will cover Baseband Ethernet only.

2.2 CSMA/CD

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the name of the protocol used on the Ethernet (802.3) bus to control the operation of the network.

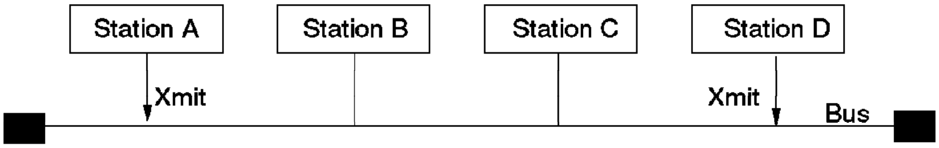


Figure 5. Ethernet CSMA/CD Bus

In a CSMA/CD bus, when a station wants to transmit data on the network bus, it first listens to see if the bus is free (that is no other station is transmitting). If the bus is available, the station starts transmitting data immediately. If the bus is not available (that is another station is transmitting), the station waits until the activity on the bus stops and a pre-determined period of inactivity follows before it starts transmitting.

If there is a *collision* after transmission (that is another station starts to transmit at the same time), the stations will stop transmitting data immediately after the collision is detected, but they continue to transmit a jamming signal to inform all active stations about the collision.

In response to this signal, each transmitting station stops transmitting and uses a binary exponential backoff algorithm to wait before attempting to transmit again. This causes each station to wait for a random amount of time before starting the whole process again beginning with the process of carrier sensing. If a station′s subsequent attempt results in another collision, its wait time will be doubled.

This process may be repeated up to 16 times, after which the station, if still unsuccessful, reports a transmission error to the higher layer protocols.

The process of *collision detection* varies according to the type of media used in the LAN. This process is described in 2.4.4, “ Medium Attachment Unit (MAU)” on page 18.

The probability of a collision occurring is proportional to the number of stations, the frequency of transmissions, size of frames and length of the LAN. Therefore, care must be exercised in designing LANs with an excessive number of stations which transmit large packets at frequent intervals. Also, you must ensure that the length of individual *segments* and total length of the LAN does not exceed a certain length as defined by the 802.3 standards. These limitations are discussed later in this topic.

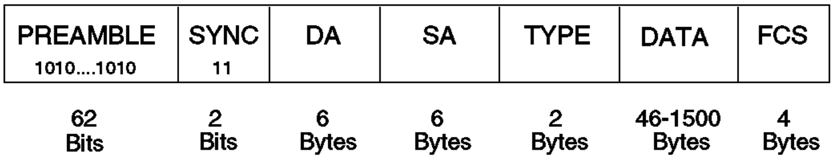
According to Ethernet and the 802.3 standard, to be able to detect collisions, a transmitting station should monitor the network for a period of time called a *slot time*. Slot time is the time during which a collision may occur and is the maximum delay for a transmission to reach the far end of the network and for a collision to propagate back. Slot time is defined to be 51.2 microseconds (512 bit times in a 10Mbps LAN). This time imposes a maximum length on the size of the network. It also imposes a minimum (64 bytes, excluding preamble and FCS) on the size of the frames transmitted by each station.

2.3 Ethernet and IEEE 802.3 Frame Formats

The frame formats for Ethernet and IEEE 802.3 are not the same. However both protocols use the same medium and access method. This means that whilst LAN stations running these protocols could share a common bus, they could not communicate with each other.

2.3.1 Ethernet Frame Format

The layout of an Ethernet frame is as follows:



PREAMBLE 1010....1010	SYNC 11	DA	SA	TYPE	DATA	FCS
62 Bits	2 Bits	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

Figure 6. Ethernet Frame Format

- PREAMBLE - 62 bits, allows the Physical Layer Signalling (PLS) circuitry to synchronize with the receive frame timing circuitry.

- SYNC (Synchronize) - 2 bits, indicates that the data portion of the frame will follow.
- DA (Destination Address) and SA (Source Address) - 48-bits, Media Access Control (MAC) address. Three types of destination addressing are supported:
  - Individual: The DA contains the unique address of one node on the network.
  - Multicast: If the first bit of the DA is set, it denotes that a *group* address is being used. The *group* that is being addressed will be determined by a higher layer function.
  - Broadcast: When the DA field is set to all 1s, it indicates a *broadcast*. A broadcast is a special form of multicast. All nodes on the network must be capable of receiving a broadcast.
- TYPE (Type Field) - 16 bits, this field identifies the higher layer protocol which is used. Vendors must register their protocols with the Ethernet standards body if they wish to use Ethernet Version 2.0 transport. Each registered protocol is given a unique 2-byte *type* identifier. As this field is used as the *length* field by the 802.3 frames, the value assigned to the *type* field in Ethernet is always higher than the maximum value in the *length* field for the 802.3. This is to ensure that both protocols can coexist on the same network.
- Data field - This contains the actual data being transmitted and is 46-1500 bytes in length. Ethernet assumes that the upper layers will ensure that the minimum data field size (46 bytes) is met prior to passing the data to the MAC layer. The existence of any padding character is unknown to the MAC layer.
- FCS - 32 bits, the result of a cyclic redundancy check algorithm (specific polynomial executed against the contents of DA, SA, length, information and pad fields). This field is calculated by the transmitting station and is appended as the last four bytes of the frame. The same algorithm is used by the receiving station to perform the same calculation and the results are compared with the contents of the FCS field in the received frame to ensure that transmission was error free.

2.3.2 IEEE 802.3 Frame Format

The layout of the IEEE 802.3 frame format is as follows:

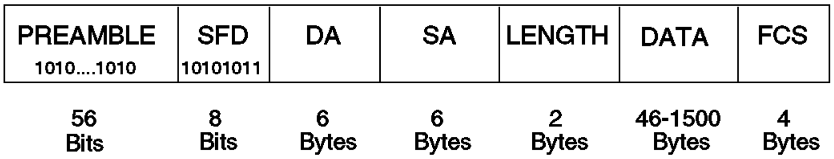


Figure 7. 802.3 Frame Format

- PREAMBLE - 56 bits, allows the Physical Layer Signalling (PLS) circuitry to synchronize with the receive frame timing circuitry.
- SFD (Start Frame Delimiter) - 8 bits, indicates that the data portion of the frame will follow.
- DA (Destination Address), SA (Source Address) - 48 bits, Media Access Control (MAC) address. Three types of destination addressing are supported:
  - Individual - The DA contains the unique address of a node on the network.
  - Multicast - If the first bit of the DA is set, it denotes that a group address is being used. The *group* that is being addressed will be determined by a higher layer function.
  - Broadcast - When the DA field is set to all 1s, it indicates a *broadcast*. A broadcast is a special form of multicast. All nodes on the network must be capable of receiving a broadcast.
- LF (Length Field) - 16 bits, indicates the number of *data* bytes (excluding the PAD) that are in the data field.
- DATA and PAD field - IEEE 802.3 (and Ethernet) specify a minimum packet size (header plus data) of 64 bytes. However, 802.3 permits the *data field* to be less than the 46 bytes required to ensure that the whole packet meets this minimum. In order to ensure that the minimum packet size requirement is met, 802.3 requires the MAC layer to add *pad* characters to the LLC data field before sending the data over the network.
- FCS - 32 bits, the results of a cyclic redundancy check algorithm (specific polynomial executed against the contents of DA, SA, length, information and pad fields). This field is calculated by the transmitting station and is appended as the last four bytes of the frame. The same algorithm is used by the receiving station to perform the same calculation and the results are

compared with the contents of the FCS field in the received frame to ensure that transmission was error free.

2.4 Ethernet (802.3) Network Model

Figure 8 shows the components of an 802.3 network and its relationship with the OSI reference model.

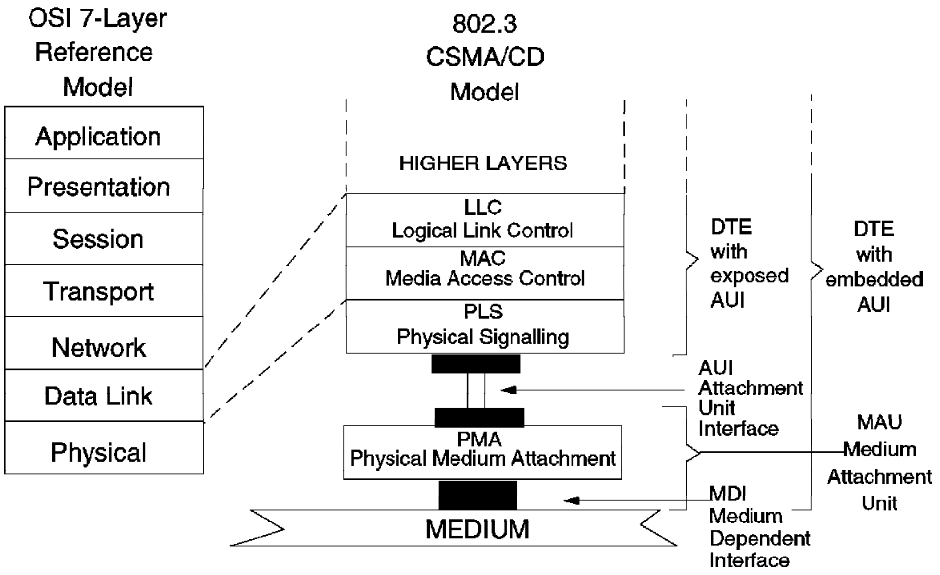


Figure 8. OSI Relationship to IEEE 802.3

In this model, *DTE* is the device that connects to the network and uses the network to exchange information with the other DTEs attached to the same network.

The following sections provide a brief description of the various components of this model.

2.4.1 Media Access Control (MAC) Sublayer

The MAC sublayer controls the routing of information between the *physical layer* and the *Logical Link Control* (LLC) sublayer by enforcing the CSMA/CD protocol. It provides:

- Frame transmission

  MAC sublayer is responsible for constructing a frame containing the data passed to it from the LLC sublayer. The transmitted frame will contain four bytes of FCS which is computed by the MAC sublayer based on the contents of DA, SA, Length field and Information field. The constructed frame will be transmitted on the physical medium.

Note

In 802.3, the data field passed to the MAC sublayer can be less than 46 bytes, in that case the MAC sublayer will append pad characters to the data field to ensure that the minimum frame size is 64 bytes before sending the data over the physical medium.

In Ethernet, a higher layer is responsible for ensuring that the data field is a minimum of 46 bytes.

- Collision detection and recovery

  To transmit the frame, the MAC sublayer must sense if the medium is currently active (in use). The status of the medium is sensed by the PLS and is passed to the MAC sublayer. If the medium is busy, the MAC sublayer will defer the transmission until the medium becomes *idle* and a period of time known as *Inter Packet Gap* expires. After this period, the MAC sublayer will start transmitting the frame. IGP is 9.6 microseconds and its purpose is to allow all the stations in the network to detect the *idle carrier*.

  If two or more stations attempt to transmit at the same time, a *collision* will occur. The collision will cause all the stations to *backoff* and restart transmission at some random time in the future as explained in 2.2, " CSMA/CD" on page 10.

- Frame recognition and copying

  When receiving a frame, the MAC sublayer identifies the Destination Address within the received frame and compares it with the address of the DTE (including Group and Broadcast addresses supported by that DTE). If a match is found, it will copy the frame, compute the FCS, and compare the result with the FCS contained in the received frame. If frame is received error free, it will be passed to the higher layers; otherwise, a *CRC Error* will be reported.

2.4.2 Physical Signalling (PLS)

PLS is part of the physical layer which resides in the DTE and provides the interface between the MAC sublayer and the *Attachment Unit Interface* (AUI). The functions provided by the PLS are:

- Transmit data output

  The frame received from the MAC sublayer will be transmitted, over the AUI cable, to the *Medium Attachment Unit* (MAU) using the *Differential Manchester Encoding* technique. This technique enables a single bit-stream to contain both the clock and the data by ensuring that there is a signal transition in the center of each bit. Also, at the bit-boundary, there is a signal transition if the transmitted bit has a value of B′1′ while there is no transition at the bit-boundary for B′0′.

- Receive data input

  PLS receives the *Manchester Encoded* data bit-stream via AUI, decodes it to NRZ format, and provides it to the MAC sublayer.

- Perform carrier sense

  The PLS is responsible for passing status of the carrier to the MAC sublayer. This will enable the MAC layer to determine if there is a network activity on the network. The PLS will inform the MAC that the carrier is active:

1. When it is receiving a frame.
2. When there is a collision on the network.
3. When the node is transmitting.

   This is used by the MAC to determine that there is an AUI and/or MAU malfunction if there is no carrier sensed during the transmission from this station.

- Perform error detection

  After each frame is transmitted, the MAU is required to send a 10 MHz signal to the DTE to inform it that the MAU is connected and functioning properly. This signal is also used to check that the collision detection circuitry within the DTE is functioning properly.

  PLS is responsible for passing the presence of this signal to the MAC sublayer. The absence of this signal from PLS, will be interpreted by the MAC as a malfunction in the MAU.

2.4.3 Attachment Unit Interface (AUI)

The connection between DTE (PLS function) and MAU (transceiver) is made by an Attachment Unit Interface (AUI) cable. This cable, which is also commonly known as the *transceiver cable*, provides the signal paths for:

- Data Out (DO) - DTE to MAU
- Data In (DI) - MAU to DTE
- Control In (CI) - Collision signal from MAU to DTE
- Power - DTE to MAU

AUI cables use individually screened AWG 22 wire for signal and power pairs. Since the 802.3 standard specifies that the DTE should have a female connector and MAU should have a male connector, the AUI cable requires opposite mating connectors to provide the connection between DTE and MAU. The connectors at the end of the AUI cable are 15-pin D-type connectors. The maximum allowed length for the AUI cable is 50 meters.

The AUI cables for Ethernet and 802.3 AUI attachment are not identical and have the following differences:

1. IEEE 802.3

   All shields of the signal pairs and the power pair are connected to pin 4. The overall AUI cable shield is connected to the AUI connector shell to provide a cable earth. Pin 1 is not used. See Figure 9 on page 17 for details.

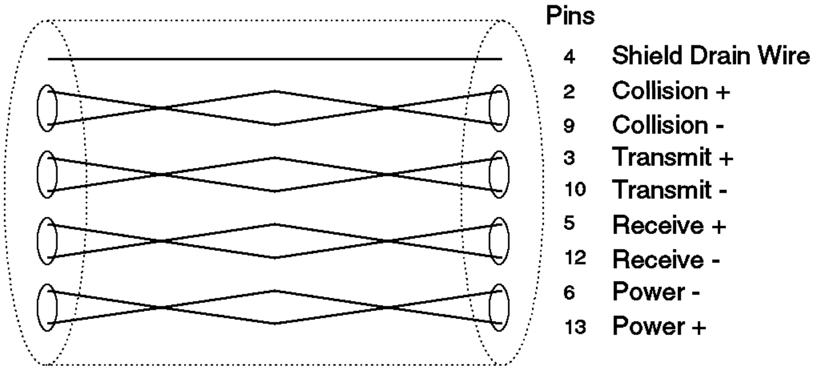


Figure 9. AUI Cable for IEEE 802.3

2. Ethernet Version 2.0

   All shields are connected to pin 1 and the AUI connector shell. Pin 4 is not used. See Figure 10 for more details.

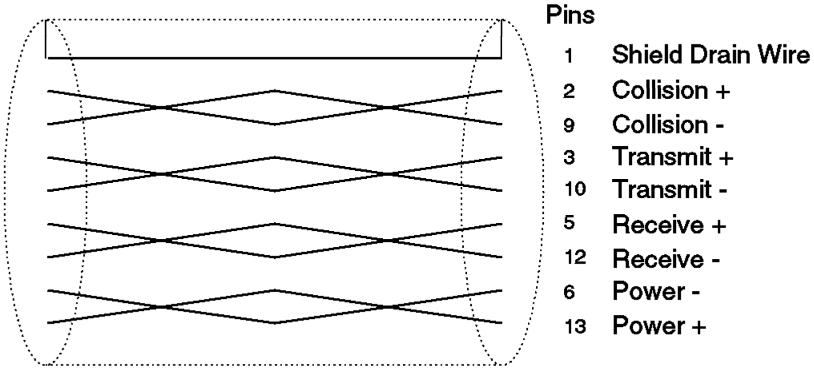


Figure 10. AUI Cable for Ethernet V2.0

3. Ethernet Version 1.0

   The point-to-point wiring of V1.0 and 2.0 is the same but the electrical requirement of the cable is different. Shielding of individual signal or power pairs is not required.

The overall AUI cable shield provides both shielding and earthing. It is connected to pin 1 and the AUI connector shell.

The gauge of wire used is AWG 22 for signal pairs and AWG 20 for power pair.

In fact most Ethernet equipment uses the Version 2 cable due to its superior construction.

2.4.4 Medium Attachment Unit (MAU)

MAUs (also known as transceivers) provide the mechanical, electrical and functional interface between the DTE and the particular media used on the Ethernet (802.3) bus. Therefore, there is a different type of transceiver for each different media type.

The use of a transceiver means that all the functions within a DTE (that is MAC, PLS and AUI) are identical regardless of the type of media used to provide the connectivity between the DTEs. The only component which requires changing, when the DTE is moved to another LAN which uses a different type of media, is the transceiver.

Transceivers perform the following functions: :

- Transmit and receive data

  The transceiver will transmit data from the DTE onto the segment. It is also responsible for receiving data from the segment and passing it onto the DTE. It is important to note that the transceiver is not an intelligent device and will pass all the data to the DTE regardless of whether it is addressed to the DTE. The transceiver does not decode the data it sends or receives.

- Collision detection

  In accordance with 802.3 rules, it is the transceiver′s responsibility to detect collisions, and to inform the DTE of their occurrence. Transceiver does this by constantly monitoring the segment and reporting back collisions. Collisions are reported via a 10MHz signal which is sent on the *Control In (CI)* pair of the AUI cable.

  The collision detection mechanism used by the MAU varies according to the type of LAN medium used. In a coax network (Thick or Thin), since all the DTEs are connected to the center conductor of the cable, the transceiver can detect two or more devices simultaneously transmitting on the network by just monitoring the *voltage level* on the center conductor. If the voltage seen is more than the allowed threshold (-1.6V nominally), there is a collision on the network.

  In a 10BASE-T network, there are two pairs of twisted copper between the DTE and the hub. One pair is for *transmit* and the other is for *receive*. During the normal transmission, the receive pair is idle. If the MAU detects activity on the receive pair while it is transmitting, it will report a collision to the DTE.

- Jabber protection

  Jabber occurs when a DTE sends more data than is allowed under the Ethernet (802.3) rules. This could be caused by hardware failure within the DTE or a running process attempting to send too large a frame. It is the transceiver′s responsibility to prevent DTE from monopolizing the network.

If a device transmits a legal size frame, it should take no more than a certain period of time to send that frame. 802.3 specification states that a transceiver must *cut off* the DTE after 20-150 microseconds by interrupting the transmission of the data on the network and indicating collision on the the *Control In (CI)* pair of the AUI cable. The transceiver should remain in this state until the DTE stops transmitting data on the *Data Out (DO)* pair of the AUI cable.

- SQE testing

  Also known as *heartbeat*, SQE test is a 10 MHz burst that is sent to the DTE by the transceiver after each frame is transmitted. The purpose is to inform the DTE that the transceiver is working properly. The SQE test signal is sent on the *Control In (CI)* pair of the AUI cable.

  > **Note**
  >
  > Repeaters must be attached to the network by transceivers that have SQE test disabled. Failing to disable SQE test will prevent the repeater from operating properly. This is because the repeater can not discriminate between SQE test and real collisions. If SQE is not disabled, the repeater will eventually partition that port and will prevent traffic from crossing the repeater.

- Link integrity

  During a normal transmission on a coax (Thick or Thin) network, a transceiver will receive its own transmissions because of the fact that all the nodes on a coax network are connected to the same center conductor on the bus. The transceiver will return this to the DTE on the *Data In (DI)* pair of the AUI cable. This signal will be used by the DTE as an indication of transmit to receive integrity.

  In networks such as 10BASE-T and 10BASE-F which have a separate transmit and receive path, the transceiver should provide an internal loopback path so that the transmitted data is received on the *receive path*. This is to ensure that the operation of various media types is transparent to the DTE and consistent network behavior is observed by the DTE across all the media types.

  However, it is still necessary in these networks, to ensure that a break in the transmit or receive path is detected. To do so, the MAU will start transmitting a *link test pulse* as soon as it has no data to transmit. If the MAU at the other end does not see either data packets or link test pulse within a predefined time known as *link loss time*, (50 to 150 microseconds for 10BASE-T), the transceiver will enter the *Link Test Fail* state. This will disable the transmit, receive, loopback, collision presence and SQE test functions. During the *Link Test Fail*, the transmission and reception of the link test pulses will continue.

  Receiving a minimum of two consecutive link *test pulses* or a single data packet, will cause the transceiver to exit the *Link Test Fail* state and re-establish the link.

2.4.5 Ethernet (802.3) Network Components

Based on the information provided so far, an Ethernet (802.3) LAN segment consists of a number of components as shown in Figure 11.

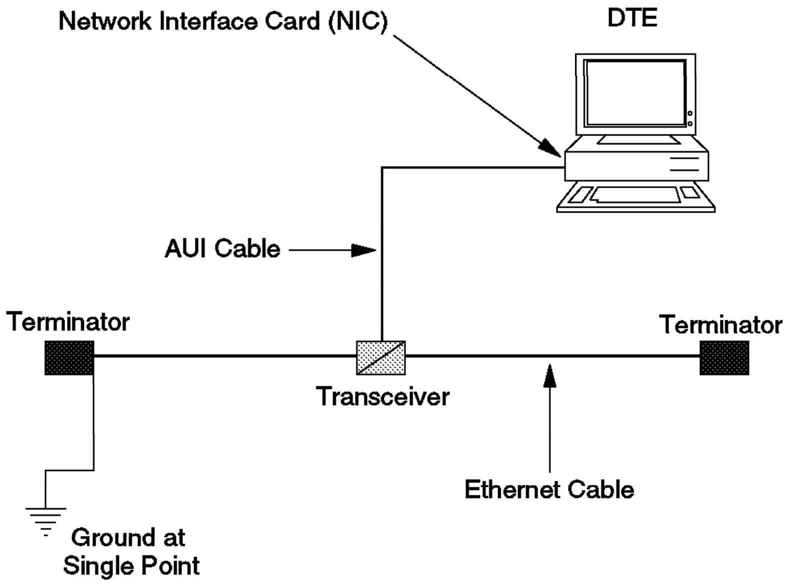


Figure 11. Ethernet Segment

A brief summary of these components is as follows:

- Ethernet Cable (bus)

  This cable provides the physical link between transceivers (MAUs). The media used can be thick or thin coax, twisted pair, or fiber optic cable.

- DTE

  These are the devices that are connected to the network. They include hosts, PCs, repeaters etc.

- Network Interface Card (NIC)

  This is the common term that is used to describe the *Network Adapter Card* that is installed on the DTE and provides the DTE with the ability to connect to an Ethernet (803) local area network. The majority of today′s adapters have onboard transceivers for at least one media type.

- Attachment Unit Interface (AUI) cable

  This is the cable which connects the NIC to the transceiver.

- Transceiver, also known as Medium Attachment Unit (MAU)

  Connects the DTE (via AUI cable) to the Ethernet (803) bus.

- Segment

  A segment is the physical bus and all transceivers (MAUs) that are attached to it.

There are various products in the market which are intended to assist the users to design networks which suit individual requirements. Some of these products are described below.

2.4.5.1 Multiport Transceivers

A multiport transceiver unit allows attachment of up to eight DTEs to a segment via a single transceiver. This is convenient when several DTEs are located close together. The advantages of using a multiport transceiver include:

1. Reduced cost (compared to 8 transceivers)
2. Ease of implementation (fewer taps onto the bus)
3. Maximize the number of DTEs on a single LAN segment

A typical multiport transceiver will have one female and eight male AUI connectors. The female port attaches to the network (via an AUI cable and a transceiver) and the male ports attach to DTEs.

Up to a maximum of two levels of multiport transceivers are permissible. See Figure 12 for an example of a network utilizing a multiport transceiver.

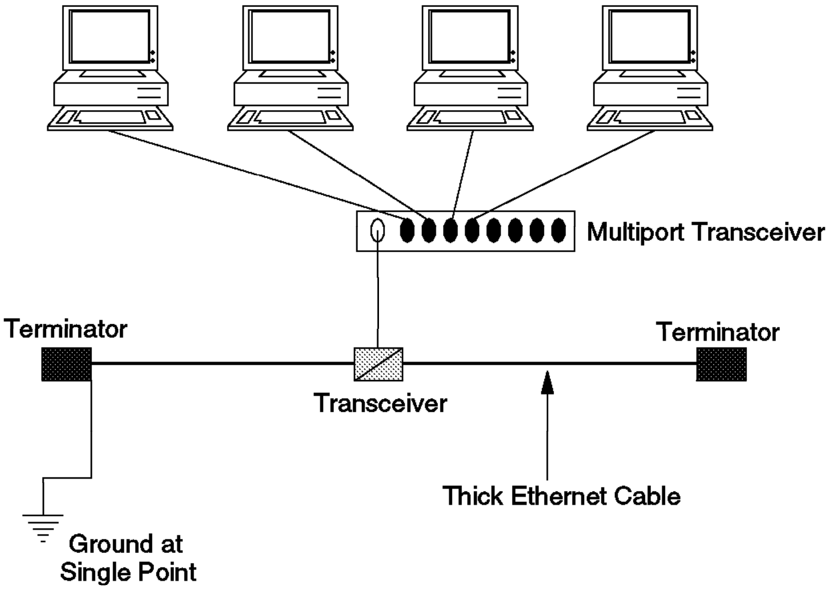


Figure 12. Multiport Transceiver

2.4.6 Repeater

As networks expand, you may need to connect two or more segments together. This may occur because:

1. The existing segment has reached its maximum length and you still need to extend the *reach* of your network by creating a new segment and connecting it to the existing segment.
2. The existing segment has reached its maximum number of transceivers (MAUs) allowed and you still need to add extra users to the network.
3. You need to interconnect two or more LANs which use different media types.

A repeater allows two (or more) separate segments to be connected together to form a single network. Segments connected in this fashion are all part of a single *Collision Domain*. Transmissions received on one port, will be sent by the repeater on all its other ports. Repeaters do not interpret, change, or act upon the data that passes through them. If a repeater detects receive activity from two (or more) ports, this constitutes a collision. In this case, the repeater will send a jamming signal on all its ports, including the active receive ports.

Repeaters are attached to the network via external or internal transceivers and are seen by the transceiver as a DTE. However, the SQE test on the transceivers connecting a repeater port to the network should be turned off; otherwise, the segment connected to that port will be partitioned by the repeater. Figure 13 shows a repeater connecting two segments. Note that these two segments can be using the same or different media types.

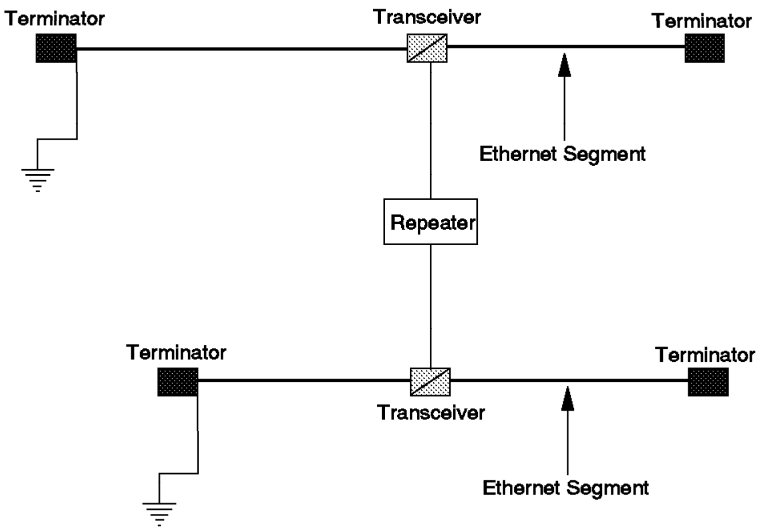


Figure 13. Ethernet Repeater

Note that Ethernet architecture limits the number of stations that can be attached to a collision domain to 1024 stations. If you reach this limit, you must use bridges to extend your network.

To prevent the shrinkage of the *Inter Packet Gap (IPG)* to a value less than the allowed minimum, there can be no more than 4 repeaters in the path between two stations in the network. This results in a maximum of 5 segments in a path, out of which only three segments can have stations attached to them. The other two segments, which are referred to as *Inter Repeater Link Segments*, consist of only two repeaters interconnected by some form of media. There are no other DTEs on an Inter Repeater Link Segment.

Note

IPG shrinkage occurs because two successive packets may experience differing bit loss on the same path. When the packet passes through a repeater, the lost preamble bits are regenerated (see below). If the first packet has experienced greater bit loss than the second, the IPG between them will shrink.

See Figure 14 for an example on an Inter Repeater Link segment.

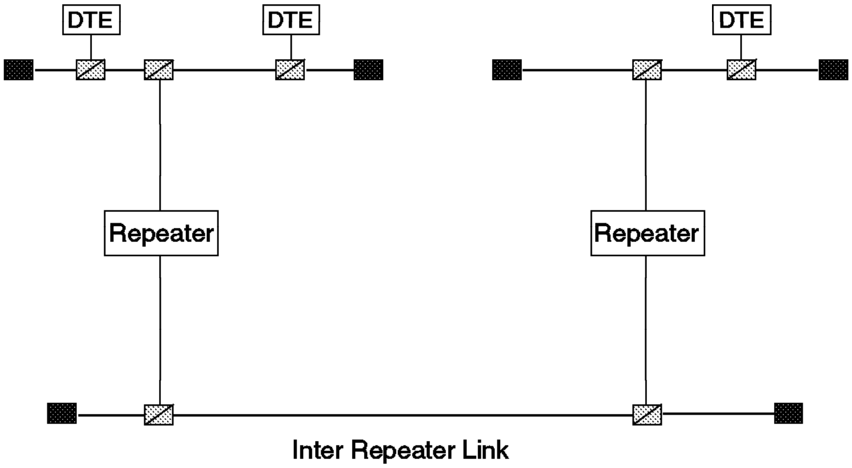


Figure 14. Inter Repeater Link

A repeater performs the following functions:

- Carrier and data repeat

  The repeater must perform the *Carrier Sense* function for all cables to which it is connected. Upon receipt of any signal at one segment, the repeater must repeat that signal on all the other segments.

- Signal regeneration

  The main restriction on the length of a segment is the signal degradation that occurs over distance. The degradation occurs because of a number of factors which affect *amplitude*, *phase* and *frequency* of the signal. Repeaters will *regenerate* and *retime* the signal to restore these properties of the signal.

- Collision detection on input

  When a repeater detects a collision on its input port, it will generate a *jamming signal* on all its output ports.

- Collision detection on output

  When a repeater detects collision on an output port, it will generate a jamming signal on all its ports.

- Partitioning and auto reconnect

  A repeater will disconnect a faulty segment from the network and will reconnect that segment only when the fault has cleared. Partitioning will occur when the repeater detects between 32 and 64 consecutive collisions or a single excessively long collision. The repeater will continue to propagate activity onto the partitioned segment, but will not act on collisions received from that segment.

  A repeater will reconnect a partitioned segment after a predetermined period of normal activity.

- Preamble regeneration

  The preamble component of a MAC frame consists of 56 bits of preamble when first transmitted. The receive circuitry within each DTE uses the preamble for synchronization. The repeater must regenerate the preamble to ensure that any lost bits within the preamble are regenerated.

- Fragment extension

  If the signal to be repeated is less than 96 bits in length, the repeater will extend the signal with artificial data so that the total number of bits output from the repeater is 96.

- MAU jabber lockup protection

  Repeaters will introduce delays into long transmissions in order to protect their own transceiver from jabber condition.

2.4.6.1 Multiport Repeater

A multiport repeater provides the same services as a normal repeater to a number of attached segments. This is shown in Figure 15 on page 25.

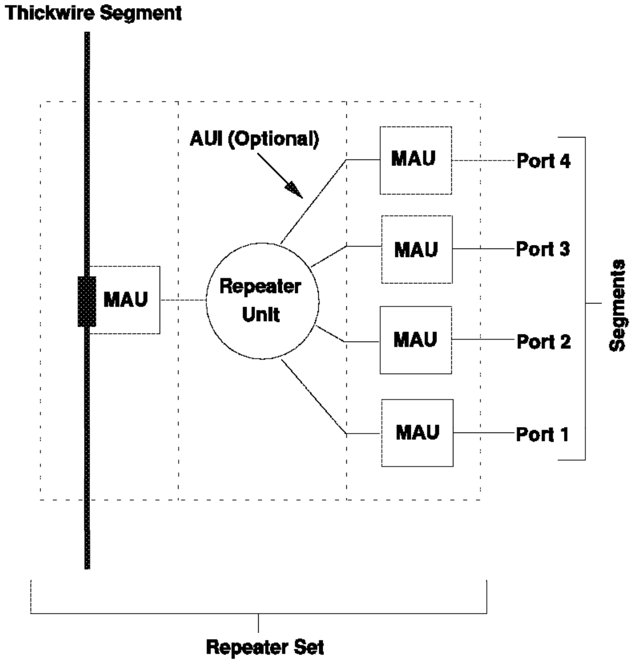


Figure 15. Multiport Repeater

2.4.7 Bridge

A bridge is used when it becomes necessary to interconnect different networks or extend an existing network beyond the limits of a single network in the following situations:

1. The network needs to be extended beyond the limits available by the use of repeaters, for example, more than 1024 DTEs on the network.
2. The required bandwidth is beyond the throughout provided by a single collision domain.
3. Connectivity is required between different LAN protocols such as Ethernet (802.3) to Token Ring.

Note that in a bridged network, each network is a separate *collision domain* and can consist of several segments connected together using repeaters. For more details about bridges, please refer to Chapter 3, “Bridging Standards” on page 45.

2.5 Ethernet (802.3) Topologies

In an Ethernet (802.3) network, various types of cables can be used to provide the physical link between the DTEs. The media used can be thick or thin coax, twisted pair, or fiber optic cable.

Thick coax is also known as 10BASE-5 or Ethernet. Thin coax is also referred to as 10BASE-2 or Cheapernet. When using coax (thick or thin), this cable acts as the bus to which the DTEs are connected. In the case of thick coax, the transceiver is an external device, while in the case of thin coax, the transceiver can be an external device or mounted onboard the adapter card (NIC).

Coax networks do not require structured wiring in the building, which makes them ideal for use in old buildings. However, they have the disadvantage of not providing management capability and fault isolation. For example, a break in the bus cable will render the whole network idle.

To enable the use of structured wiring in an Ethernet environment, a standard known as 10BASE-T has been developed which provides a point-to-point link between the DTE and a central *hub* over twisted pair wiring. The hub contains MAU function on each of its ports. It also contains a repeater function which allows these point-to-point segments to communicate with each other. The hubs can also be connected to each other to extend the size of the network and the number stations that can be attached to them.

Because, of the existence of hub(s), a 10BASE-T network provides a much better management and fault isolation capability than the coax-based networks.

Fiber optic cables are used to provide point-to-point links, typically as a *backbone* between concentrators, to interconnect buildings or cross long distances within a building. However, it is also possible to use fiber optic cables as a means of providing connections to workstations. There are various standards covering the use of fiber optic cables in an Ethernet (802.3) environment. These standards are described briefly in the following sections.

The physical size of a network and the number of stations attached to it varies according to the type of medium used to construct the network. However, users can build a network consisting of mixed topologies by using repeaters and bridges. Also, such mixed topologies are made possible by intelligent hubs such as the IBM 8250 which provide various repeater, bridge, media and management functions via a number of modules which can be installed on the hub as required. The following sections provide a brief description of the various standards used in Ethernet (802.3) networks.

2.5.1 10BASE-5 (Thicknet)

The names given to the IEEE 802.3 standards provide some information as to the capabilities and requirements of the implementation. In the case of 10BASE-5 they have the following meaning:

10	indicates the data rate	(10Mbps)
BASE	indicates the transmission type	(Baseband)
5	indicates the maximum cable length	(500 Meters)

10BASE-5 (thicknet) use a very high quality coaxial cable for the bus. This cable is very thick (10 mm in diameter) which makes it difficult to manipulate particularly if it is being run into work areas and needs to go in and out of ducting. The cable is generally marked every 2.5 meters to indicate where transceivers can be attached.

Attachment of DTEs to the coaxial cable is done by attaching a transceiver to the cable and attaching the DTE to the transceiver via an (AUI) cable. This is shown in Figure 16.

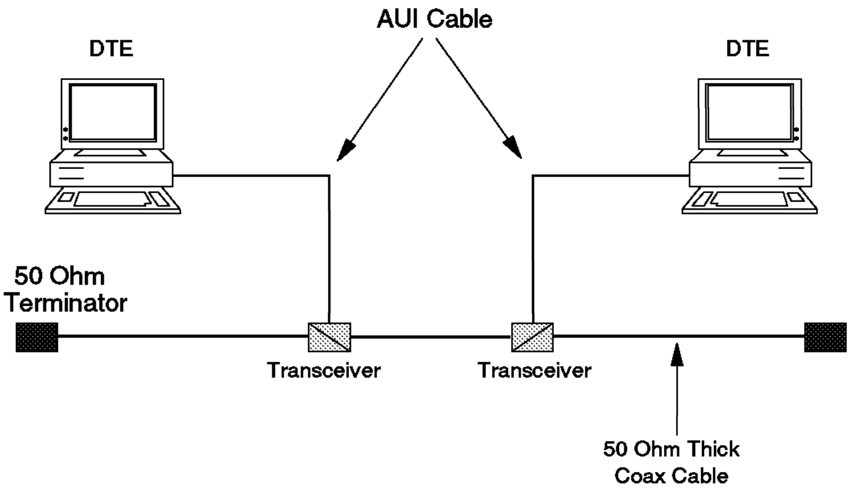


Figure 16. 10BASE-5 Segment

Note that terminators are used at both ends of the segment to prevent the signal from being reflected back when it reaches the end of the segment.

The transceivers used with this type of installation come in two main types:

1. Piercing Tap Connectors or Vampire Taps

   These are the most common type used on 10BASE-5 networks. They are known as *vampire taps* because the center connection is made by drilling or piercing through the outer shield and dielectric of the cable and inserting a tap screw.

   Making this type of connection is not a trivial task. This makes adding/removing transceivers a job for a skilled person. Figure 17 on page 28 shows a cross section of a tapped thicknet cable.

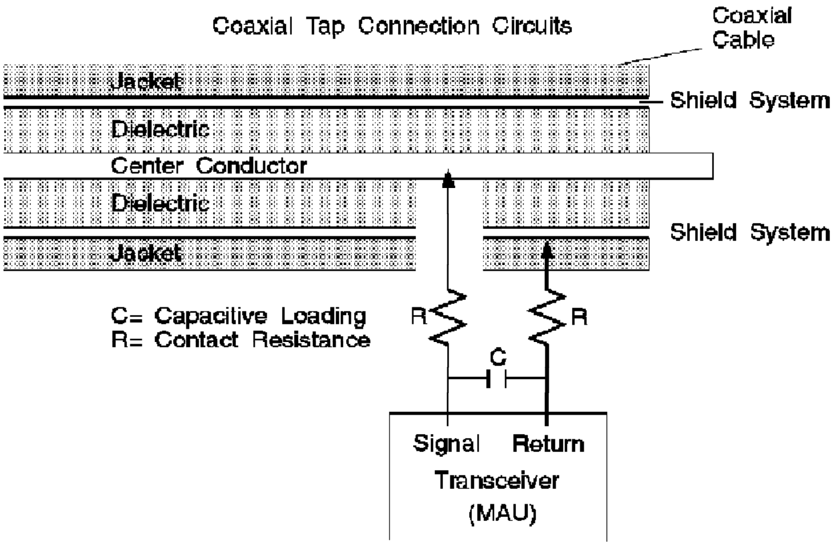


Figure 17. Cross Section of Tapped Thicknet Cable

2. N Type Connector

   This type of connection requires the cable to be segmented. As cutting the cable, while the bus is in operation, renders the network unusable, these transceivers are not as common as the *vampire tap*. However, as manufacturing techniques have improved, various manufacturers do offer 10BASE-5 segmented cables terminating in N connectors and transceivers capable of being attached via this method.

In modern environments 10BASE-5 topology is not very practical. The difficulties of manipulating the bus cable, rerouting AUI cables, attaching transceivers etc., means that installations of this nature are inherently inflexible and unable to accommodate the rate of change that is expected on most local area networks today.

Despite the drawbacks associated with this type of installation, 10BASE-5 has been widely installed. The use of multi-port transceivers with a thinner and more flexible 5 meter transceiver cable made it somewhat easier to add/remove DTEs and enable most connections to be made without having to manipulate the thick coaxial cable. Also, despite the fact that 10BASE-5 has become less popular for providing access to the LAN directly it is still widely used particularly in situations where relatively few attachments are required and change is limited.

Table 1 provides a summary of the 10BASE-5 specification.

Table 1 (Page 1 of 2). 10BASE-5 Specification

Item	Specification
Cable Type	Ethernet 50-ohm PVC or teflon FEP coaxial
Connectors	N-series

Table 1 (Page 2 of 2). 10BASE-5 Specification

Item	Specification
Termination	Segment ends not attached to repeaters must be terminated with 50 ohm terminators
Transceiver Cable	Four-stranded, twisted-pair conductors with an overall shield and insulating jacket
Data Rate	10 Megabits/sec
Max segment length	500 meters
Distances between transceivers	2.5 meter multiples
Max no. of transceivers	100 transceivers
Max no. of stations per network	1024 adapters
Max transceiver cable length	50 meters
Impedance	50 ohms (+/- 2)
Attenuation	8.5 dB for 500 meters at 10 MHz
Max Propagation Delay/segment	2165 nanoseconds
DC resistance	5 ohms per segment

2.5.2 10BASE-2 (Thinnet/Cheapernet)

As a means of addressing the problems associated with 10BASE-5, the 10BASE-2 standard was defined.

The name 10BASE-2 was chosen because of the characteristics of this type of network as shown below:

10	indicates the data rate	(10Mbps)
BASE	indicates the transmission type	(Baseband)
2	indicates the maximum cable length	(200 Meters)

Note that the actual length permitted on a 10BASE-2 segment is 185 meters.

10BASE-2 uses a much lower grade of coaxial cable than 10BASE-5. The cable is also a lot thinner and more flexible which makes it easier to manipulate and capable of being brought right up to the DTE. This, in conjunction with the fact that the 10BASE-2 transceiver function is generally integrated into most of the Ethernet adapters, provides the user with the option to connect the DTE to the bus directly and avoid the use of AUI cable. However, because of the lower quality of the cable, there is a reduction in both the segment length available and number of transceivers supported when compared to 10BASE-5.

A 10BASE-2 network consists of a number of thin coax cables connected to each other via a number of T-connectors. In addition to connecting the two cables together, a T-connector provides a BNC connection for attaching the DTE. The use of BNC type connectors makes adding and removing transceivers a straightforward task in a 10BASE-2 network. Figure 18 on page 30 shows an example of a typical 10BASE-2 network.

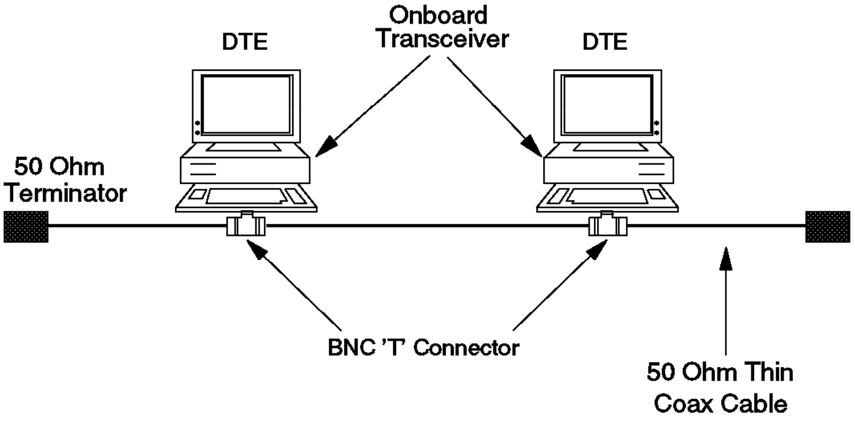


Figure 18. 10BASE-2 Segment

Note that terminators are used at both ends of a segment to prevent the signal from being reflected back when it reaches the end of the segment.

Table 2 provides a summary of the 10BASE-2 specification.

Table 2. 10BASE-2 Specification

Item	Specification
Cable Type	RG-58A/U, 50-ohm coaxial cable
Connectors	BNC type
Termination	Segment ends not attached to repeaters must be terminated with 50 ohm terminators
Transceiver cable type	Four-strand, shielded twist-pair conductors with overall shield and insulating jacket.
Data Rate	10 Megabits/sec
Max segment length	185 meters
Min distance between transceivers (or T-Connectors)	0.5 meter
Max no. of transceivers/Segment	30 transceivers
Max transceiver cable length	50 meters
Max no. of stations per network	1024 adapters
Impedance	50 ohms (+/- 2)
Attenuation	8.5 dB for 185 meters at 10 MHz
Max Propagation Delay/Segment	950 nanoseconds
DC resistance	10 ohms per segment

Because of the relative simplicity of running and attaching stations to it, 10BASE-2 is often used to extend the services offered by an existing 10BASE-5 network.

The advantage of 10BASE-5 in terms of the segment length available can be utilized for parts of the LAN where change will be minimal such as through ducts and risers to provide a backbone bus.

The advantage of 10BASE-2 in terms of the cable itself being easier to manipulate plus the relative ease with which transceivers can be added and removed can be utilized in areas of the LAN where changes will be made more frequently to the configuration of the network.

Repeaters and/or bridges must be used to connect the segments.

2.6 10BASE-T

During the 1980s, due to the fall in the cost of hardware, the concept of a workstation on every desk became a reality and many businesses became dependent on the need to attach these workstations to local area networks to enable them to exchange information with the other workstations and provide them with access to the available services within the organization. This stretched implementations of 10BASE-5/10BASE-2 networks to their limits. Manufacturers of the attachment devices came up with numerous ingenious ways of making these systems more flexible but could not hide the fact that the basic requirement of connecting the workstations in series was incapable of providing the flexibility needed.

It was also becoming clear that a more structured approach to the whole subject of providing services into the business environment was required. Many organizations were discovering that a majority of buildings were not able to make provisions for business services such as telephone, telex, fax, data and video adequately.

A number of companies were marketing structured cabling systems designed to provide a single cabling infrastructure over which most services could be provided. These were mainly star-wired systems, in which the cabling radiated from a wiring closet to service a defined area within the building. The wiring closets were also linked together to allow services to be connected between any two points in the building.

The EIA/TIA (Electronics Industries Association/Telecommunications Industries Association) brought out a standard for the physical cabling of buildings to provide data and voice services. This provides the standards for:

- Topology - structured wiring using a star topology between the work area and the wiring closet.
- Maximum cabling distance (point to point) between the wiring closet and the work area.
- Recommended media and connectors. For example:
  - 100 Ohm Unshielded Twisted Pair (UTP) consisting of four 24 AWG wire pairs.
  - 8-pin modular jack and plug such as RJ-45 pairs.

- 150 Ohm Shielded Twisted Pair (STP) consisting of two individually shielded pairs and a common shield around both pairs.
- Media connector as specified in the IEEE 802.5 standard.

The standard also provides recommendations for the use and application of fiber and coaxial cables within the building.

The 10BASE-T standard was defined by IEEE to address the requirement of running Ethernet/802.3 over the structured cabling systems using twisted pair copper wires. Although, actually completed prior to the EIA/TIA 568 standard, a 10BASE-T Ethernet (802.3) LAN requirement would be met by a cabling system that conformed to EIA/TIA 568.

The term 10BASE-T was chosen for this standard because:

10	indicates the data rate	(10Mbps)
BASE	indicates the transmission type	(Baseband)
T	indicates the medium	(Twisted Pair)

10BASE-T is a star topology in which the DTEs are attached to a central *hub*. The hub acts as a multiport repeater between a number of segments in which each segment is a point-to-point connection between a DTE and a port on the hub.

A segment can also be a point-to-point connection between two hub ports. This would allow you to set up a network consisting of multiple hubs. Also, by taking advantage of bridges and repeaters (which normally are offered as modules which can be installed on these hubs), networks consisting of mixed topologies of 10BASE-T 10BASE-5, 10BASE-2, etc. can be constructed.

Table 3 provides a summary of the 10BASE-T specification.

Table 3. 10BASE-T Specification

Item	Specification
Cable Type	2 Unshielded Twisted-pairs (UTP)
	0.4 mm AWG 26
	0.5 mm AWG 24 (most widely used)
	0.6 mm AWG 22
Connectors	RJ-45
Termination	No external terminators are required
Data Rate	10 Megabits/sec
Single segment length	100 meters (point-to-point)
Max no. of repeaters/segment	2 multiport repeaters
Impedance	85 - 111 ohms (nominal 100)
Attenuation	8.5 - 10 dB for 100m at 10 MHz
Max. Propagation Delay/Segment	1000 nanoseconds

2.6.1 FOIRL and 10BASE-FL

Fiber Optic Inter Repeater Link (FOIRL) was the first standard to be defined for the use of fiber optic cables in an Ethernet LAN. Although it was originally intended as a repeater-to-repeater link only, providing a long-distance connection of up to 1 km between two repeaters, it has also been used to allow fiber connectivity to the desktop.

The use of FOIRL for desktop connectivity was originally excluded from the standard, but the 10BASE-FL standard, which is specified to supersede FOIRL, permits such connections.

FOIRL is similar to the 10BASE-T standard. It requires the use of a separate transmit and receive path. It also requires the use of repeaters in a central hub acting as the concentration point for a group of nodes.

Similar to 10BASE-T, an FOIRL MAU is required to perform link integrity. FOIRL link integrity is performed by each MAU transmitting a 1 MHz signal when no data transmission is taking place. If the MAU at the other end fails to detect this signal it enters *Link Fail* state and prevents the DTE from transmitting onto the network.

10BASE-FL extends the allowable distance between two MAUs to 2 km.

2.6.2 10BASE-FB

10BASE-FB is designed to provide a superior technology using synchronous signalling over the fiber cables. A 2.5 MHz active idle signalling is used to indicate that the transmit path is idle. In addition, the transmit data from the repeater is synchronized to this idle signal, enabling the receiving MAU to remain locked to the active/idle packet data transition.

2.7 Token-Ring

The token-ring network is a local area network (LAN) which runs at a speed of 4 or 16 Mbps. The token-ring network uses a token-passing protocol. In a token-passing protocol, a ring station can only transfer data to the ring while it is holding a token. The token is a specific bit sequence (24 bits) circulating around the ring at a speed of 4 or 16 Mbps.

A token-ring network uses one of several twisted pair media specifications, each having its own price/performance ratio, and all suitable to carry most other data communications signals.

The IEEE 802.5 and the ISO 8802-5 standards describe the token-ring media access protocol and its physical attachments.

In a token-ring network the stations on the LAN are physically connected to a wiring concentrator in a star-wired ring topology. Logically, stations are connected in a pure ring topology. Each station has transmitter as well as receiver circuitry. Figure 19 on page 34 shows a sample ring configuration.

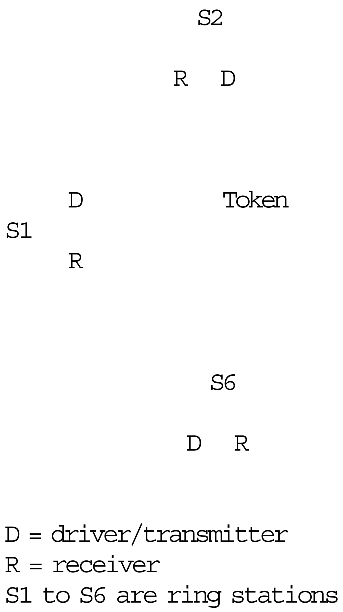


Figure 19. Sample Ring Configuration

Access to the ring is controlled by a circulating token. A station with data to transmit waits for a free token to arrive. When a token arrives, the station changes the token into a frame, appends data to it and transmits the frame. If the destination station is active, it will copy the frame and set the *frame copied* and *address recognized* bits, providing MAC level acknowledgment to the transmitting station. The sending station must strip the frame from the ring and release a new token to the ring.

An option in the architecture allows the sending station to release a token immediately after transmitting the frame trailer, whether or not the frame header information has already returned. This is called *early token release* and tends to reduce the amount of idle time in higher speed token-passing rings running at 16 Mbps.

The token-passing protocol provides an extensive set of inherent fault isolation and error recovery functions, for implementation in every attaching device. The adapter network management functions include:

- Power-on and ring insertion diagnostics
- Lobe insertion testing and online lobe fault detection
- Signal loss detection, beacon support for automatic test and removal
- Active and standby monitor function
- Ring transmission error detection and reporting
- Failing component isolation for automatic or manual recovery

In summary, the token-passing ring protocol is based on the following cornerstones:

- Active monitor (a station elected by the token claiming process)

  - Ensures proper ring delay
  - Triggers neighbor notification
  - Monitors token and frame transmission
  - Detects lost tokens and frames
  - Purges circulating tokens and frames from the ring
  - Performs auto-removal in case of multiple active monitors
- Standby monitor (any other ring station)

  Detects failures in the active monitor and disruptions on the ring
- Token claiming process

  A new active monitor is elected when the current active monitor fails. This process can be initiated by the current active monitor or by a standby monitor.

The token-passing protocol provides for efficient use of the media under both light and heavy traffic loads. It guarantees fair access to all participating stations. This fairness is enhanced by an eight-level priority mechanism, based on priority reservations made in a passing token or frame. A key benefit of the token-passing ring protocol is its ability to handle increased traffic loads or peaks, without penalizing the existing users, making it an ideal protocol for larger and/or more heavily used LANs. This also makes it a good base for connection to even higher bandwidth LANs such as FDDI.

As token-ring architecture and design has been extensively covered by many other IBM publications, we limit our discussion of token-ring to the above summary. Readers unfamiliar with token-ring are advised to consult the Token-Ring Network Architecture Reference (SC30-3374).

2.8 FDDI

In 1982 the American National Standards Institute (ANSI) created the X3T9.5 committee, which began studies on high-speed communications. Originally envisioned as a standard for high-speed host channels, FDDI rapidly became viewed as a new generation of LANs which will use optical fiber to provide a high-speed communication network.

Today, it is possible to implement standardized FDDI LANs based on the physical backgrounds and the logical links which are defined in the ISO 9314 and the ANSI X3T9.5 standards. The ANSI X3T9.5 and ISO 9314 committees describe FDDI as a dual counter-rotating ring which operates at a rate of 100 Mbps (million bits per second). In many ways, FDDI is similar to the IEEE 802.5 token-ring, although there are some differences. FDDI uses a token-passing protocol in which each station has the chance to transmit data when a token passes. A station can decide how many frames it will transmit using an algorithm which permits *bandwidth* allocation. FDDI also allows a station to transmit many frames without releasing the token.

An FDDI network consists of a set of stations/devices connected to each other as a serial string of stations/devices by a transmission media to form a physically closed loop. Information is transmitted sequentially, as a stream of suitably encoded symbols, from one active station/device to the next active one. Each station/device regenerates and repeats each symbol. The method of actual physical attachment to the FDDI network may vary and is dependent on specific application requirements.

FDDI uses two rings:

- The *primary ring*, which is similar to the main ring path in token-ring terminology.
- The *secondary ring*, which is similar to the backup ring path of a token-ring.

Note each ring consists of a single fiber path which is equivalent to a pair of copper conductors.

FDDI permits many attachment units (stations, concentrators, and bridges) to be attached in various ways.

From a wiring point of view, FDDI is similar to a fiber optic token-ring network; however, there are the following differences between the token-ring and FDDI techniques:

- A device can be attached directly to the ring without requiring a concentrator such as the Multistation Access Unit (MAU) on a token-ring.
- A device can be attached to either or both of the primary/secondary rings.

To differentiate between devices that attach to one ring or both rings, FDDI defines two classes of devices:

- A *Class A* device attaches to both of the rings directly. It may be a station and it is called a Class A station or a Dual Attachment Station (DAS). It can be a concentrator and it is called a Dual Attachment Concentrator (DAC).
- A *Class B* device attaches to only one of the rings directly or through a concentrator. It may be a station and it is called a Class B station or a Single Attachment Station (SAS). It can be a concentrator and it is called a Single Attachment Concentrator (SAC).

Concentrators are active devices that act as *wiring hubs* and are similar to an active token-ring access unit (such as an IBM 8230 Controlled Access Unit).

During normal ring operation, the primary ring is active while the secondary ring is idle.

In the wake of a failure on the primary ring, the secondary ring will become active when a Class A station or a Dual Attachment Concentrator wraps the primary ring to the secondary ring establishing a single ring. This functionality is mandatory to maintain the reliability of the LAN.

2.8.1 FDDI over Copper

An alternative to FDDI is Shielded twisted pair Distributed Data Interface (SDDI). This proposal is for transmitting FDDI directly on copper wires without converting the electrical pulse stream to optical signals. The data stream remains at the rate of 100 Mbps.

This type of solution is envisioned to provide a copper-based FDDI solution which could be implemented on the existing cabling system and will cost approximately less than 50% of the equivalent fiber solution. The IBM 8240 FDDI Wiring Concentrator, the IBM 8250 Intelligent Hub and the PS/2 FDDI Workstation Adapter are examples of available products built to this SDDI specification.

There is also a proposal to the ANSI FDDI TP-PMD workgroup for a copper solution running FDDI over UTP category 5.

2.8.2 Port Types

The type of ports at the ends of a physical connection determine the characteristics of that connection. These characteristics include whether the connection will be accepted or rejected.

The standard specifies four port types for FDDI ports:

- A-Type

  For Dual Attachment Stations: Primary Ring-In, Secondary Ring-Out

- B-Type

  For Dual Attachment Stations: Secondary Ring-In, Primary Ring-Out

- M-Type

  On a Concentrator, to attach a Single Attachment Station

- S-Type

  On a Single Attachment Station, to attach to a Concentrator

The connection rules for the different port types are the following:

- A-to-B and B-to-A are peer-to-peer trunk connections
- M-to-S is a master to slave connection
- M-to-A and B provides dual homing
- S-to-S is a point to point connection

In a dual ring configuration, one end of the link is configured as an A-Type and the other end as a B-Type port. When configured as a tree, one end of the link is an M (Master) port and the other end is an S (Slave) port.

Only Dual Attachment Stations (DAS) reside on both rings. Single Attachment Stations (SAS) reside on the FDDI tree and connect to the network via concentrators. In this case, the concentrator can be a DAC or a SAC.

Table 4 shows the connection rules for Single and Dual Attachment Stations.

Table 4 (Page 1 of 2). Connection Rules for SAS and DAS

Port Type	Port Type	Rule
A	A	Undesirable peer connection that creates twisted primary and secondary rings.
A	B	Normal trunk ring peer connection.
A	M	Tree connection with possible redundancy. Port B shall have precedence for connecting to port M in a single MAC node.
A	S	Undesirable peer connection that creates a wrapped ring.
B	B	Undesirable peer connection that creates twisted primary and secondary rings.
B	M	Tree connection with possible redundancy. Port B shall have precedence for connecting to port M in a single MAC node.

Table 4 (Page 2 of 2). Connection Rules for SAS and DAS

Port Type	Port Type	Rule
B	S	Undesirable peer connection that creates a wrapped ring.
M	M	Invalid configuration.
M	S	Normal tree connection.
S	S	Connection that creates a single ring of two slave stations.

2.8.3 Dual Attachment Station Ring

Figure 20 on page 39 shows an FDDI dual ring configuration consisting of Dual Attachment Stations (DAS). Each station will have both ports (A and B) attach to the rings. The cabling between the stations has to be all fiber or shielded twisted pair (STP).

The FDDI network consists of the primary ring on which the data flows from port B on one station to port A on next station, and the secondary ring in which the data flows in the opposite direction of the primary ring. The secondary ring provides the backup path for failure conditions. In normal conditions, there is no data flow on the secondary ring.

If any station fails, the ports on the adjacent stations will wrap the primary and secondary rings and the network will continue to operate as a single ring. For example, in Figure 20 on page 39, if station 1 fails, station 4 will wrap its B port and station 2 will wrap its A port, resulting in a single ring which connects the remaining stations (2, 3 and 4).

If there is a failure on the cabling, the stations at either end of the broken cable will wrap their corresponding ports to restore the operation of the ring. For example, in Figure 20 on page 39 if the main ring between station 1 and station 4 is broken, the A port on station 1 and the B port on station 4 will wrap and all four stations will continue to operate on the same FDDI ring. However, if there was a second break on the ring (for example between stations 2 and 3) then the ring would be fragmented, forming two rings, one with station 1 and 2, and another with stations 3 and 4.

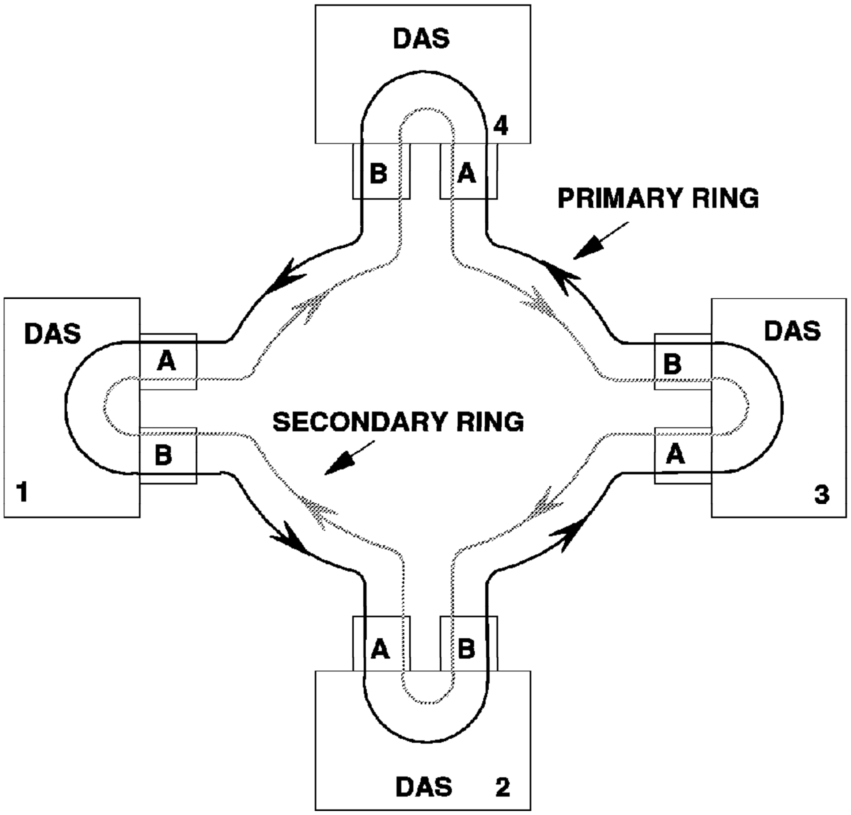


Figure 20. FDDI Dual Attachment Station Ring

2.8.4 Dual Attachment Concentrator Ring

Figure 21 on page 40 shows an FDDI Dual Attachment Concentrator ring. In this configuration, the signal will enter the concentrator at the A port and after flowing through the M ports, it will exit the concentrator at the B port.

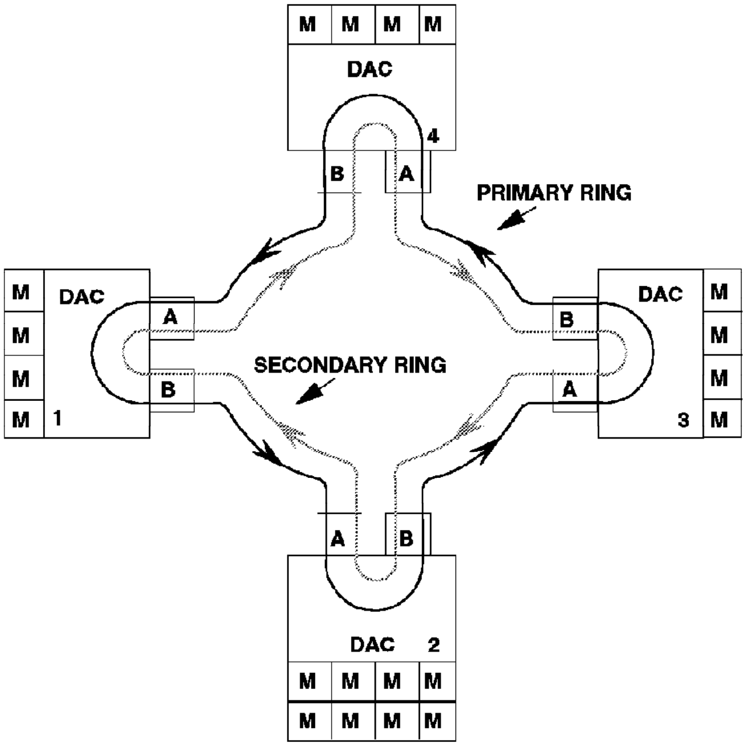


Figure 21. FDDI Dual Attachment Concentrator Ring

2.8.5 Dual Attachment Concentrators and Workstations

Figure 22 on page 41 shows the topology of workstations attached to a Dual Attachment Concentrator (DAC). Each workstation is attached as a Single Attachment Station (SAS) to the master port (M) of a concentrator (DAC). The M port attaches each SAS to the primary ring.

Data enters each DAC from the A port and after passing through each M port (and its attached workstation) exits through the B port.

The benefit of a concentrator attachment is that it allows a SAS to enter and leave the ring without the risk of disrupting the ring.

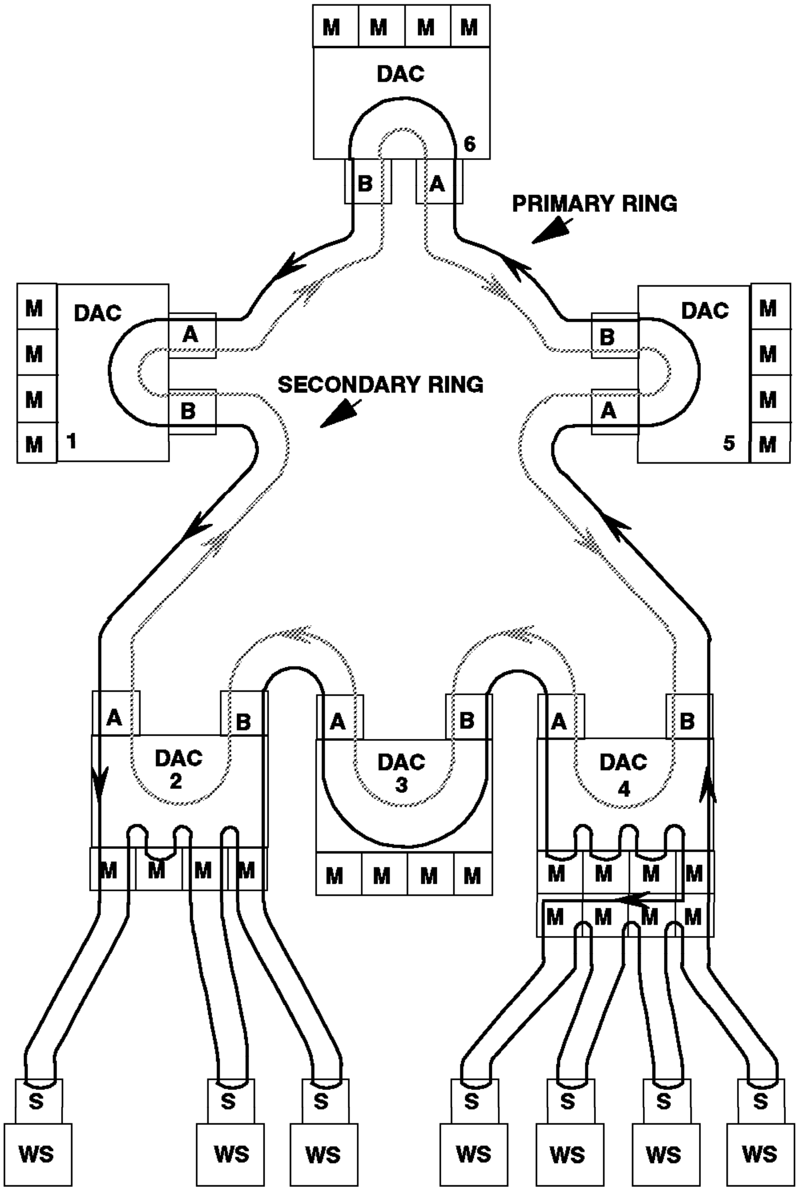


Figure 22. Dual Access Concentrator and Workstations

2.8.6 Tree Topology

Figure 23 on page 42 shows an FDDI tree topology. The purpose of the diagram pictured here is to show the signal flow through a complex tree topology. It is not intended to suggest a typical installation.

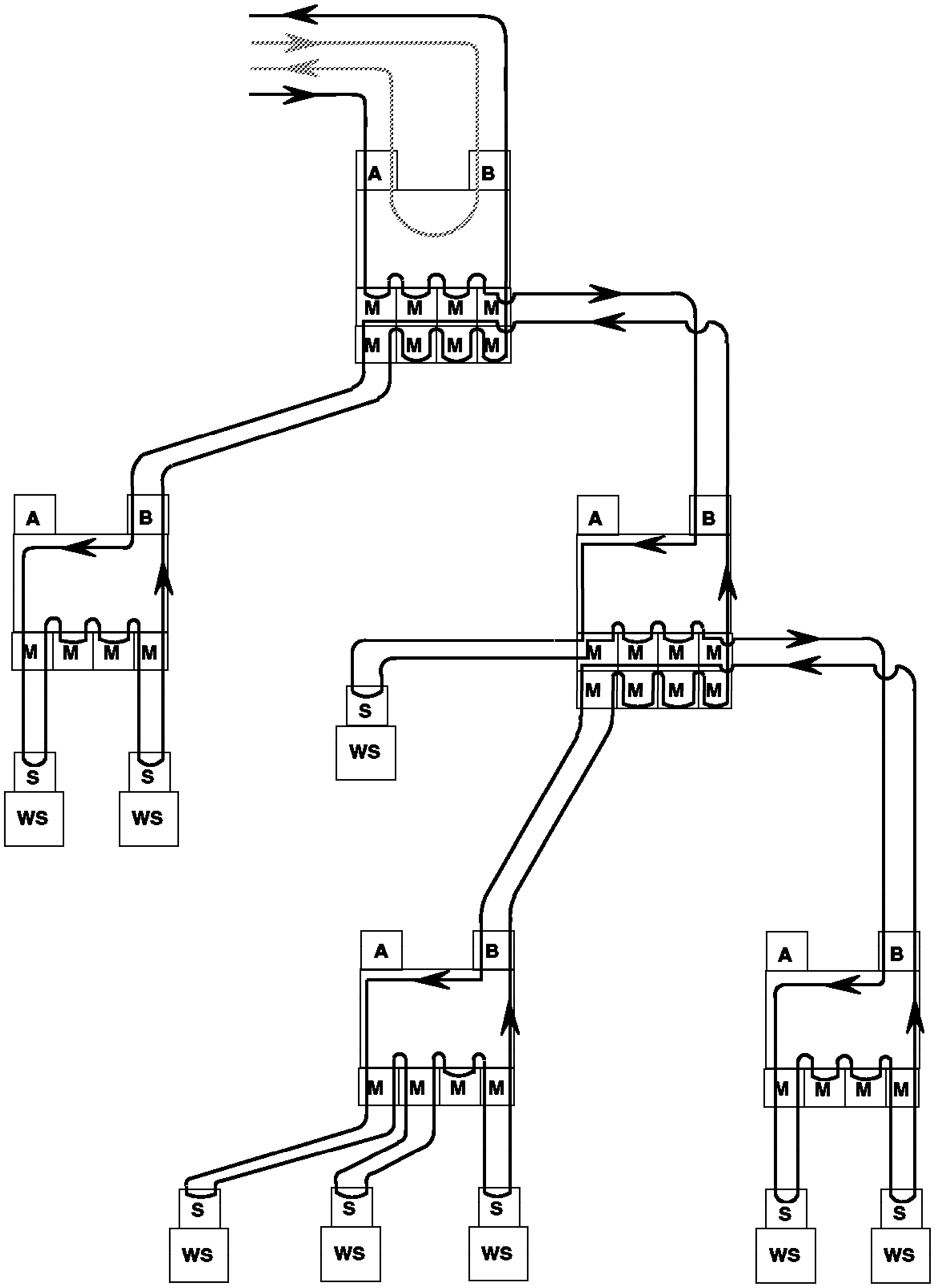


Figure 23. FDDI Tree Topology

2.8.7 Dual Homing

Figure 24 shows an FDDI *dual homing* topology. A concentrator, that is not part of the main ring, may be dual attached via one or two other concentrators to provide greater availability. When connected in this manner, a concentrator is described as a Dual Homing Concentrator (DHC).

Similarly a Dual Attachment Station can be connected to one or two concentrators using both A and B ports to provide high availability. The station connected in this manner is considered a Dual Homing Station (DHS).

In both of these cases, only port B is active, and the connection to port A remains in standby mode. Should the connection to port B fail, port A would become active without any impact on the users of the Dual Homed Station or Concentrator.

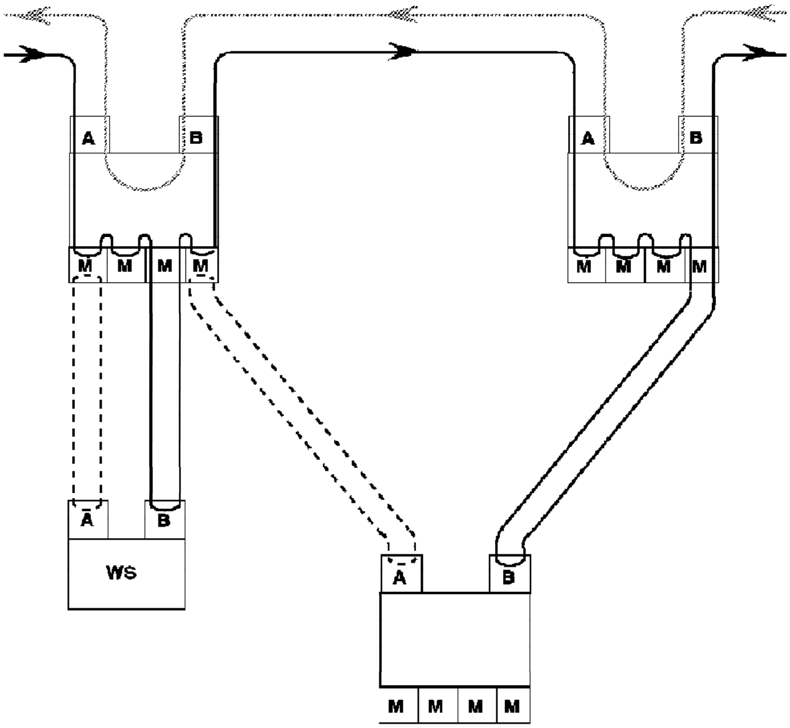


Figure 24. FDDI Dual Homing Topology

Chapter 3. Bridging Standards

Often, local area network requirements exceed the capabilities of a single ring or bus and thus the need to divide them to smaller LANs and to connect them together using bridges or routers. In general, the reasons to use bridges could be one of the following:

- Maximum number of stations has been reached

  For example, token-ring architecture allows a maximum of 260 stations on a ring while Ethernet architecture allows a maximum of 1024 stations in a single collision domain.

- Physical network size.

  Need to extend local area network capability beyond the cabling guidelines for a single segment.

- Amount of traffic.

  The available bandwidth of a LAN must be shared by all stations. The more stations that there are, and the more stations that are attempting to transmit, the smaller the share of bandwidth for each station.

To provide for the bridging requirements, different bridging standards have been developed. This chapter discusses the standards for:

- Transparent bridging
- Source Route bridging
- Source Route/Transparent bridging

Also, some of the implications of mixing various bridging standards within the same logical network is explored.

3.1 Internetworking and the OSI Reference Model

The industry and the standards bodies have chosen to give distinct names (*bridges, routers and gateways*), to subnetwork connectors, depending on the layers at which they are used.

The following is a brief description of these subnetwork connectors in terms of the 7-layer OSI reference model:

1. **Gateways** operate above layer 3 and support protocol conversion between unlike protocol stacks. As an example, the communication between OSI and SNA or OSI and TCP/IP is handled by a gateway.
2. **Routers** work at layer 3. They interconnect and route across many physical subnetworks, including LANs and WANs.
3. **Bridges** operate at layer 2. They can be used to connect homogeneous and heterogeneous LANs. For example, a bridge can be used to connect two token-ring LANs or connect a token-ring LAN to an Ethernet LAN.
4. **Repeaters** operate at the physical layer and are used to extend the physical characteristics of the subnetwork. Repeaters can sometimes also provide media conversion between optical fiber and copper.

In a token-ring environment, repeaters are used to extend the distance between wiring closets while in an Ethernet environment, they are used to connect two or more Ethernet segments. For more information about Ethernet repeaters, see 2.4.6, “Repeater” on page 21.

The relationship of internetworking devices to the seven-layer OSI reference model is shown in Figure 25.

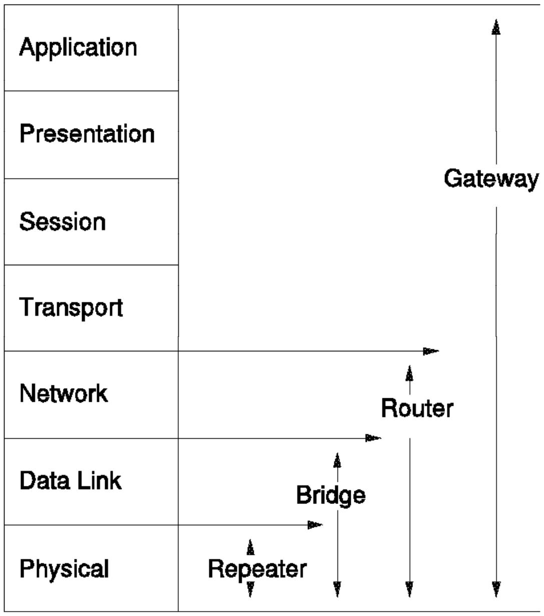


Figure 25. OSI Reference Model and Internetworking Devices

3.2 Bridging Methods

The following types of bridges exist today:

Transparent Bridges

These bridges forward frames based on the destination address. If the destination address of a frame is known to be on the same LAN as the source address, then no forwarding will take place. If the destination address is not known on the same LAN as the source address, then the bridge will forward the frame. The IEEE standard 802.1d defines the operation of transparent bridges. These bridges are predominantly used with Ethernet LANs. However, they may be used with other LAN types such as token-ring.

Source Routing Bridges

These bridges are used to provide interconnection between 802.5 LANs. They forward frames based on a *Routing Information Field* (RIF) which is part of the MAC frame header. The RIF defines the route that a frame will take to get from source to destination.

SR-TB Bridges
The Source Routing to Transparent Bridge translates between Source Routing (SR) and Transparent Bridging (TB). An example is the IBM 8209 Token-Ring to Ethernet Bridge. There is no standard for SR-TB bridge operation.

SRT Bridges
The Source Route Transparent bridge is able to perform Source Route Bridging and Transparent Bridging simultaneously. The IEEE 802.1d base document plus Appendix C to this document defines the standard for the SRT bridge operation.

Details of these bridging methods are discussed later in this chapter.

3.3 Bridge Operation

Bridges operate at the Media Access Control (MAC) layer, which is the lower sublayer of the Data Link Control (DLC) layer. A bridge consists of two (or more) physical and MAC layer connections (one for each LAN segment they interconnect). The MAC layer functions contained in the bridge are interconnected by a relay function which passes frames received from one MAC to the other MAC if certain conditions are satisfied.

Note

The relay function may also provide protocol conversion if the interconnected MAC protocols are different.

MAC layer bridges are generally transparent to the users of the Data Link Control (DLC) layer. Due to this transparency to higher layers, MAC layer bridges may serve multiple higher layer protocols such as SNA, NetBIOS and TCP/IP concurrently.

Because a bridge is generally *invisible* to higher layer protocols, there are certain considerations that should be taken into account when designing a multi-segment LAN. Some of these considerations are:

- Do not inadvertently duplicate MAC addresses in interconnected LANs.
- Bridges forward all layer 2 broadcasts, with a potential danger of broadcast storms with certain protocols.
- Protocols that are connection-oriented at layer 2 must receive end-to-end acknowledgments within a time window. Using multiple bridges and/or remote bridges may result in these timers to expiring, resulting in the termination of the session.

3.4 Transparent Bridging

As mentioned earlier, the transparent bridging method is mainly used to connect Ethernet LANs. However, it can also be used to interconnect other types of LANs such as token-ring. With transparent bridging the protocol is contained entirely within the bridge. This makes the operation of the bridge totally *transparent* to the end-stations. The end-stations are not aware of the presence of the bridge and view all the interconnected LANs as a single LAN.

There are two key points about transparent bridges:

1. They need a filtering database for the decision to forward/discard a frame.
2. They allow only one active path between a pair of interconnected LANs. This is necessary to prevent frames from looping in the network and is realized by a so-called *spanning tree algorithm*.

3.4.1 Filtering Database

Once operational, a transparent bridge builds a filtering database by listening to the frames exchanged on the LAN and learning the addresses of the stations attached to any LAN. It does this by recording the source addresses of the frames seen on the LANs connected to each of its ports which is in forwarding state (forwarding state will be discussed later in this topic). This results in the creation of the dynamic part of the filtering database. An aging mechanism ensures the removal of addresses which are not seen for a predetermined period of time. The timeout period is determined by the *aging time* parameter which is a user-definable option.

The filtering database also contains static entries. These static entries are divided into required and a optional support.

Required support

- IEEE reserved addresses, which the bridge must discard. This includes the *Bridge Group Address* (X′800143000000′) which is used in the *spanning tree Hello BPDU*. See 3.4.3.1, “Filtering Database Update” on page 55.

Optional support

- Can be set by the user to provide customized forwarding and/or blocking of a frame or group of frames. For example, if a frame is received on port 1, forward on ports 2 and 4 but not on port 3.

In general, a transparent bridge applies the following rules to determine if a frame should be forwarded or discarded:

- If the destination address (DA) is associated with the receiving port, then the frame is discarded.
- If the DA is associated with specific port which is in the forwarding state, the frame is forwarded.
- If the DA is not associated with a specific port, the frame is forwarded on all ports of the bridge which are in forwarding state.

Note that user-definable filters can be used to affect the forwarding/discarding of frames.

In the example shown in Figure 26 on page 49, a two-port bridge is shown with its filtering database. The bridge knows that the destination address of PC B is on the rightmost port. Therefore, it will forward any frame on LAN1 which is destined to this station while it discards all the frames on LAN2 addressed to PC B.

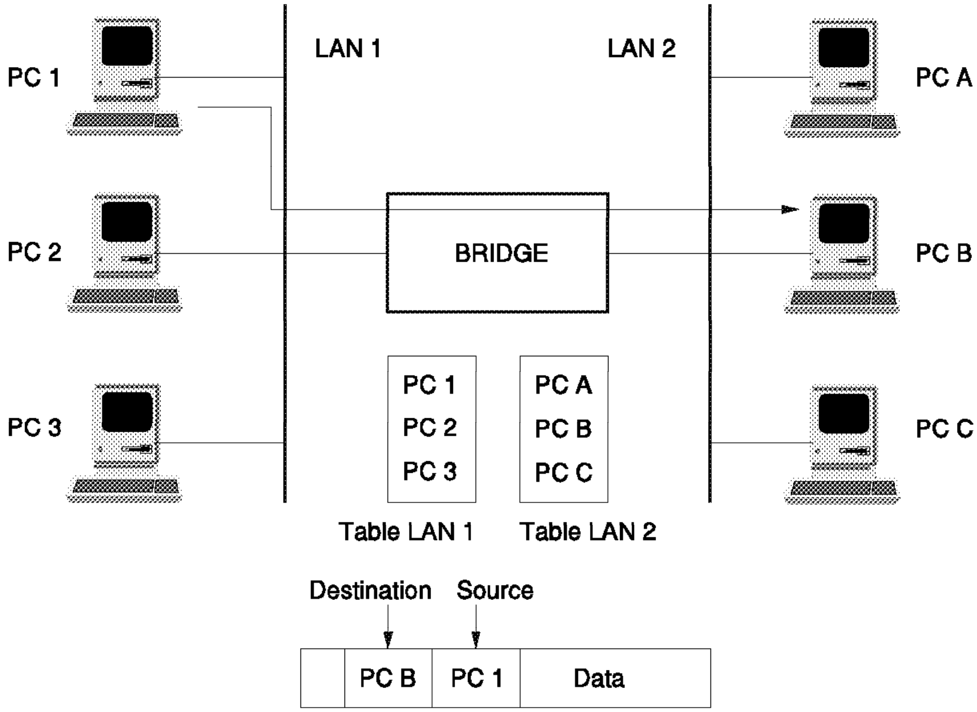


Figure 26. Transparent Bridge Operation

3.4.2 The Spanning Tree

The spanning tree algorithm enables transparent bridges to dynamically discover a loop-free network and provide a single physical path between any two stations attached to the network.

If there is more than one bridge between any two interconnected LANs, the spanning tree algorithm will ensure that only one of them will be included in the spanning tree. This bridge will be in so-called *forwarding* state and is the only one which will be passing frames between the two interconnected LANs. All the other bridges which are parallel to the forwarding bridge will be excluded from the spanning tree and will not perform any frame forwarding. These bridges are said to be in *blocking* state.

Note that in the case of multi-port bridges, a single bridge may be in forwarding state on some of its ports while it is in blocking state on the others.

Figure 27 on page 50 shows an example of the spanning tree used to provide the bridging between several interconnected LANs. The upper part of the diagram shows the physical network and the lower part of the diagram shows the spanning tree and the status of the various bridges in the network.

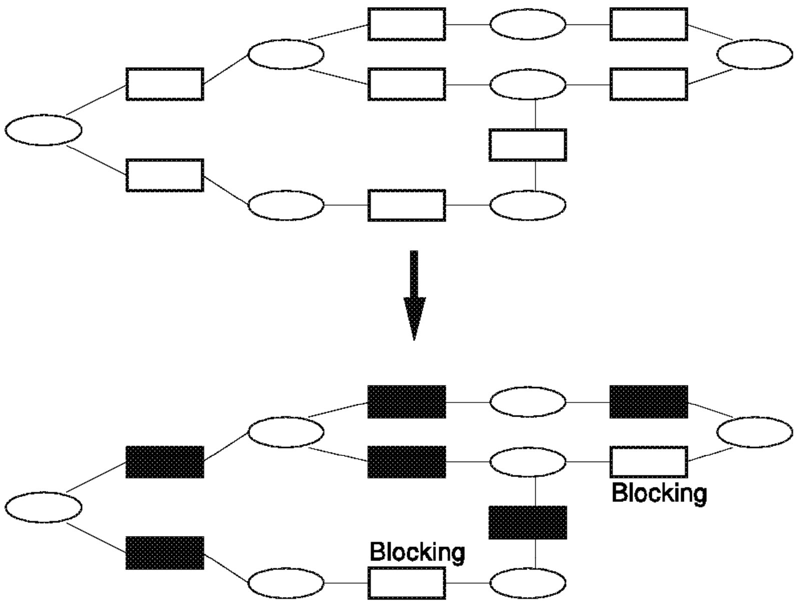


Figure 27. Forming a Spanning Tree

To set up the spanning tree, bridges transmit to each other a special configuration message called *Configuration Bridge Protocol Data Unit* (BPDU). This is also referred to as the *Hello* BPDU and is used by the bridges to:

1. Choose a single bridge on the network to be the **root bridge**. This is the bridge with the lowest *bridge identifier* in the network.

   The bridge identifier is comprised of a two-byte *bridge priority* followed by a six-byte *bridge address*. The bridge priority is a configuration parameter. The bridge address is the MAC address of one of the bridge ports and its purpose is to ensure that bridge identifier is unique.

2. Choose one port on each bridge as the **root port**. This is the port that has the *lowest cost path* to the root bridge.

3. Elect a **designated bridge**, for each LAN in the network, from among the several bridges that may be residing on that LAN. The elected bridge is the one that offers the lowest cost path from the stations residing on that LAN to the root bridge. The port on a designated bridge attached to the LAN for which the bridge is designated becomes the **designated port**. Note that in a multi-port bridge, there may be more than one designated port.

4. The root port of the designated bridge enters the **forwarding** state.

5. The designated port(s) on each designated bridge enters the **forwarding** state.

6. All other ports remain in **blocking** state.

See 3.4.2.2, “Hello BPDU” on page 53 for details about the contents of the Hello BPDU.

3.4.2.1 The Spanning Tree Protocol

To participate in the spanning tree protocol, each bridge will initially assume it is the root bridge and will transmit a Hello BPDU on each of its ports. This message will be sent every **Hello Time**. Hello time is one of the spanning tree configuration parameters that can be specified for each bridge during the bridge configuration. This Hello BPDU will have the following characteristics:

1. Source address will be the address of the transmitting bridge
2. Destination address will be X′800143000000′.
3. Source and destination SAPs will be X′42′.
4. The Root ID field will contain the ID of the transmitting bridge.
5. The Bridge ID field will contain the ID of the transmitting bridge.
6. The Path Cost field will contain 0.
7. It will be sent out by the bridge on all its ports.

Each Hello BPDU sent out on a bridge port will be received by all the other bridges which are connected to the LAN attached to that port.

Each bridge uses the information received in the Hello BPDUs to determine the root bridge, the designated bridges and the designated ports within each designated bridge. To do this, each bridge will continue transmitting its Hello BPDU on each of its ports until it receives a *better* Hello BPDU than the one it is transmitting on that port.

The better Hello BPDU will be determined based on the following information contained in the Hello BPDU (listed in order of their significance):

1. The lowest Root ID
2. The lowest Path Cost to the bridge
3. The lowest transmitting Bridge ID
4. The lowest Port ID

As soon as a bridge receives such a Hello BPDU on a port, it will stop transmitting any further Hello BPDUs on that port and will use the information received in the *better* Hello BPDU to transmit a new Hello BPDU on all its other ports. The new Hello BPDU will have the following characteristics:

1. Source address will be the address of this bridge.
2. Destination address will be X′800143000000′.
3. Source and Destination SAP will be X′42′.
4. The Root ID field will contain the Root ID received in the *better* Hello BPDU.
5. The Bridge ID field will contain the ID of this bridge.
6. The Path Cost field will be the sum of the path cost received in the *better* Hello BPDU plus the path cost defined for the bridge port on which the *better* Hello BPDU was received.
7. It will be sent out by the bridge on all its ports except the port on which the *better* Hello BPDU was received.

This process will be repeated by all the bridges until:

1. There is one bridge (root bridge) remaining who is still transmitting its original Hello BPDU.
2. One bridge (designated bridge) on each LAN is transmitting the Hello BPDU based on the Hello BPDU received from the root bridge.

On the designated bridge, the port on which the best Hello BPDU is received is the *root port* and all the ports onto which the Hello BPDUs are transmitted are the *designated ports*.

Note

There may be some ports on the designated bridge, over which the bridge will not be transmitting Hello BPDUs due to the fact that the received BPDUs on those ports are better than the one this bridge would be able to transmit (but they are not better than the Hello BPDU received on its root port).

Once the root and designated bridges have been elected, the root ports and the designated ports will be put in forwarding state and all the other ports will be put in blocking state.

Figure 28 shows the how the spanning tree algorithm is used to determine root bridge, designated bridges and designated ports. In this example, the letter ″p″ shows the bridge priority and the letter ″c″ shows the path cost assigned to the ports attached to each LAN segment.

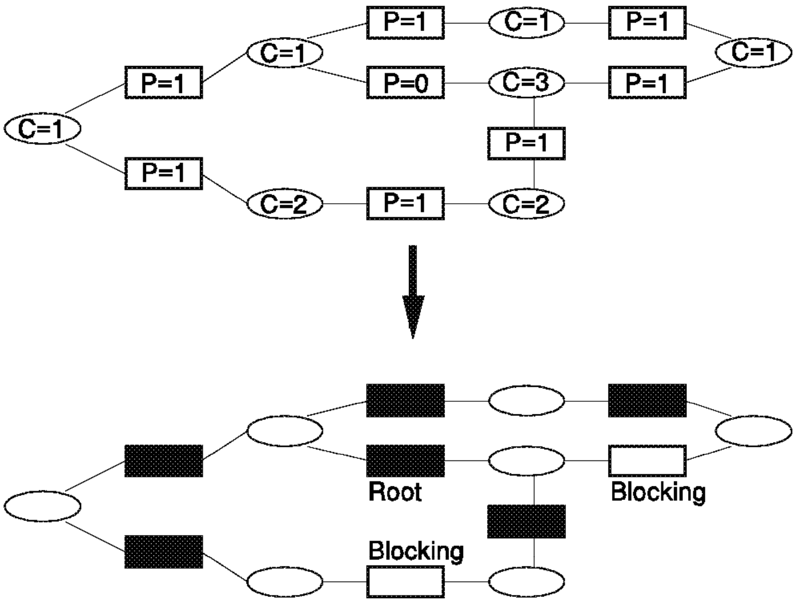


Figure 28. Spanning Tree Algorithm

3.4.2.2 Hello BPDU

The format of the Hello BPDU is shown in Table 5.

Table 5. Configuration BPDU

Field	Size (bytes)
Protocol Identifier	2
Protocol Version Identifier	1
BPDU Type	1
Flags	1
Root Identifier	8
Root Path Cost	4
Bridge Identifier	8
Port Identifier	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

The meaning of the various fields in the Hello BPDU are as follows:

- Protocol Identifier

  Identifies the spanning tree protocol. This field contains 0.

- Protocol Version Identifier

  Identifies the version number of the spanning tree protocol used. This field contains 0. Note that the IEEE 802.1d committee has proposed Version 1 for *remote* bridges only.

- BPDU Type

  Denotes the type of BPDU. This field contains 0 for a configuration (Hello) BPDU and 128 for Topology Change Notification (TCN) BPDU. See 3.4.3, “Transparent Bridges and Network Topology Changes” on page 54.

- Flags

  – Topology Change

    This is the lease-significant bit of the Flag field and if set to 1, denotes that the receiving bridge should use the *forward delay timer* rather than the *aging timer* for aging out the entries in the filtering database. See 3.4.3.2, “Topology Change Notification” on page 55 for more details about Topology Change Notification.

  – Topology Change Acknowledgment (TCA)

    This is the most-significant bit of the Flag field and if set to 1, it indicates that the bridge no longer needs to send TCN BPDUs. See 3.4.3.2, “Topology Change Notification” on page 55 for more details about TCA.

- Root ID

  Specifies the bridge identifier of the root bridge. This field consists of the *priority* of root bridge (2 bytes) and *bridge address* of the root bridge. Priority is assigned to a bridge during the configuration and bridge address is the MAC address of the port with the lowest port identifier.

- Root Path Cost

  Total cost from the bridge that transmitted this BPDU, to the root bridge. BPDUs transmitted by the root bridge will contain 0 in this field.

- Bridge ID

  Bridge ID of the bridge transmitting the Hello BPDU. This field consists of 2 bytes of the bridge priority followed by the MAC address of the port with the lowest port identifier. The bridge transmitting a Hello BPDU is either the root or a designated bridge.

- Port Identifier

  Port priority (1 byte) plus the port number (1 byte). Port priority is a user configurable option.

- Message age

  Indicates the approximate age of the BPDU since it was originated by the root bridge.

  When a bridge receives a Hello BPDU, it starts a timer which is incremented every second. The initial value of this timer is the value contained in the *message age* field of the received BPDU.

  When the designated bridge transmits its own Hello BPDU, it puts the value of this timer in the Message Age field.

- Max age

  This is the time after which the Hello BPDU stored in the bridge is deleted. Once the Message Age timer has reached this value, the bridge will assume the root bridge is not active and it will begin to establish itself as the root bridge.

- Hello time

  Denotes the frequency with which the root bridge should send the Hello BPDUs. This is a user-configurable option.

- Forward Delay Time

  Specifies the length of the time that the bridge should stay in each of the *listening* and *learning* states before moving from blocking to forwarding state. As discussed in 3.4.3.1, “Filtering Database Update” on page 55, this timer may also be used for aging out the entries in the filtering database.

3.4.3 Transparent Bridges and Network Topology Changes

Bridges using the spanning tree algorithm automatically adjust to the changes in network topology to ensure that a loop-free network is maintained. A change in the network topology happens:

1. Bridges enter or leave the network.
2. Possibly when spanning tree parameters change causing bridge ports to change state or causing a change in the choice of the root bridge.

The result of any of the above changes is that:

1. The spanning tree has to be reconfigured using Topology Change Notification protocol.
2. The Filtering database must be updated.

3.4.3.1 Filtering Database Update

A transparent bridge builds a filtering database, for each of its ports, by listening to the frames exchanged on the LAN attached to that port. This database contains the addresses of stations attached to that LAN segment and are used to forward/discard frames across the bridge.

When the network topology changes due to the bridge addition/removal/reconfiguration, it is important that the bridges can update their filtering database quickly enough to cope with these changes in a manner that:

1. It ensures the stations can continue to communicate with each other through the bridges.
2. The performance of the network is not affected due to the bridges forwarding the frames incorrectly and flooding the network.

To ensure the above, an *aging timer* is used by the bridges to delete the entries within the filtering database, which have not been used recently.

This timer should be able to cope with changes which happen as a result of stations physically moving from one LAN to another, as well as changes happening as a result of a bridge addition/removal (spanning tree reconfiguration). The latter, normally will result in a group of stations logically moving from one LAN to another.

In general, to cope with the changes occurring due to the station moves, a longer aging timer is required than the one required to cope with the spanning tree reconfiguration. Therefore, the standard defines two timer values for the aging timer:

1. A longer timer value is to be used in coping with normal changes due to station addition/removals/timeouts. This is a user-configurable parameter and is referred to as *aging time*.
2. A shorter timer value to be used when the bridge is in a state of topology change. See 3.4.3.2, “Topology Change Notification.” The *forward delay timer* of the root bridge is used for this purpose.

   Note that the forward delay timer is specified for each bridge during its configuration, but all the bridges will use the value defined in the current root bridge.

3.4.3.2 Topology Change Notification

Spanning tree topology change is detected by a bridge whenever:

- A port enters *forwarding* state,
- A port leaves *forwarding* state or
- A new bridge becomes the root bridge

When a topology change happens, the following actions will be performed:

1. The bridge detecting the change issues a Topology Change Notification (TCN) BPDU. This frame will be sent on the root port to the destination address X′800143000000′.
2. The designated bridge on this port will acknowledge this frame by sending back a Hello BPDU with Topology Change Acknowledgment (TCA) set to 1.
3. The designated bridge will issue, on its root port, its own TCN BPDU.

4. This process repeats until a TCN BPDU reaches the root bridge.

5. The root bridge will start transmitting a Hello BPDU with the TCN set to 1 for a period equal to the sum of forward delay time and max age time.

6. The bridges which receive the Hello BPDU with TCN set to 1, will start using the shorter aging timer (forward delay) for aging out filtering database entries. The forward delay timer will be used as the aging timer until a Hello BPDU with TCN set to 0 is received.

Figure 29, shows an example of the effect of an active bridge failure or removal. The spanning tree protocol will be used to reconfigure the spanning tree as shown in the lower part of Figure 29.

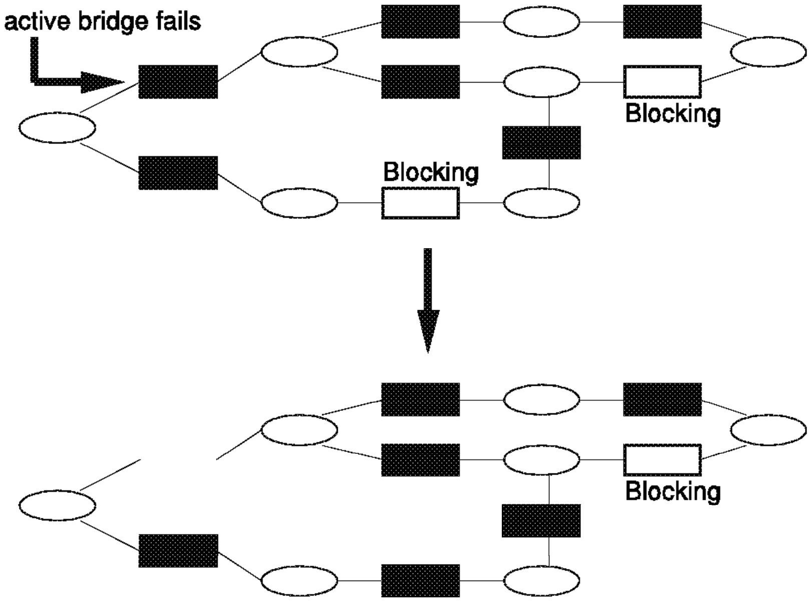


Figure 29. Reconfiguration of a Spanning Tree

3.4.3.3 Spanning Tree Parameters

Table 6 shows the configurable spanning tree parameters which are defined as part of the standard for transparent bridging.

Table 6 (Page 1 of 2). Spanning Tree Parameter

Parameter	**Meaning**	**Default**
Bridge Max Age	Maximum age of received BPDU	20 seconds
Bridge Hello Time	Time interval between Configuration BPDUs	2 seconds
Bridge Forward Delay	Time spent in Listening state, Time spent in Learning state, short aging timer	15 seconds
Bridge Priority	Priority portion of bridge identifier	32768
Path Cost	Cost for entering this port	1000/LAN_speed (Mbps)

Table 6 (Page 2 of 2). Spanning Tree Parameter

Parameter	Meaning	Default
Port Priority	Priority portion of port identifier	128

3.4.3.4 Transparent Bridge Port States

The ports on a transparent bridge can be in one of the following five states:

Disabled Not participating in spanning tree protocol, not learning, not forwarding frames.

Blocking Participating in spanning tree protocol, not learning, not forwarding frames.

Listening Participating in spanning tree protocol, not learning, not forwarding frames, in transition from blocking to learning. The purpose of this state is to prevent the bridge from building its filtering database, based on incorrect station information, before the spanning tree becomes stable.

Learning Participating in spanning tree protocol, learning, not forwarding frames. The purpose of this stage is to minimize the unnecessary forwarding of frames by ensuring that the bridge has built-up its filtering database before beginning to forward frames.

Forwarding Participating in spanning tree protocol, learning and forwarding frames.

All of the above states, except the disabled state, are determined by the spanning tree protocol.

3.4.3.5 The Spanning Tree Summary

The result of the spanning tree algorithm for transparent bridges, is a loop-free network in which the end-stations require no knowledge of the network topology to be able to communicate with the other stations through one or more bridges. But, the result is also a network in which there is no load balancing over bridges and in case of parallel bridges all but one of the bridges will be idle (blocking state).

3.5 Source Route Bridging

Source route bridging is the scheme used by IBM Token-Ring bridges to control the route a frame will traverse in a multisegment LAN. Source routing bridges put the responsibility of *navigating* through a multisegment LAN on the end-stations. This is in contrast to transparent bridging in which the end-stations have no knowledge of the route a frame will travel to reach its destination.

In a source route bridging environment, the route through the network is described by the sequence of *rings* and *bridges* that the frame should traverse to reach its destination. This information is stored in the *Routing Information Field* (RIF) of a token-ring frame.

RIF is an optional part of the MAC header of the token-ring frame. The presence of this optional field in the MAC frame is indicated by the *Routing Information*

Indicator (RII) bit which is the high order bit (″Individual/Group″ bit) of the source MAC address. If set to 1, it signals the existence of the RIF in the frame.

If present, the RIF contains at least a 2-byte *Routing Control Field* and optionally may contain up to a maximum of 8 *Route Designator* fields.

Each Route Designator field is two bytes in length and consists of *ring number* (12 bits) and *bridge number* (4 bits).

The Routing Control field specifies if the frame is non-broadcast, single-route broadcast or all-route broadcast. It also specifies the length of the RIF and the largest frame size which can be sent over this path. In addition, *direction bit* of this field, indicates whether the Route Designators are to be interpreted from left-to-right or from right-to-left.

The Route Designators map out the route through a multisegment LAN by specifying the sequence of rings and bridges that the frame will traverse.

Figure 30 on page 59 shows details of RIF and RII fields carried in a token-ring frame.

The broadcast indicators in the Routing Control field also control the way a bridge treats the frame. The types of source-routed frames are:

Non-Broadcast also known as *routed* frames. The frame will travel a specific route as defined in the RIF.

All-Routes Broadcast also known as *general broadcast* frames. The frame will be forwarded across the bridge provided certain conditions are met. These conditions are described later in this chapter.

Single-Route Broadcast also known as *limited broadcast* frames. The frame will be forwarded by all bridges that are configured to forward single-route broadcast frames. If the network is configured properly, a single-route broadcast frame will appear once on each LAN segment.

Typically all-routes broadcast and single-route broadcast frames are used to discover a route during session setup. Once the route is established, non-broadcast frames are generally used.

3.5.1 Route Determination

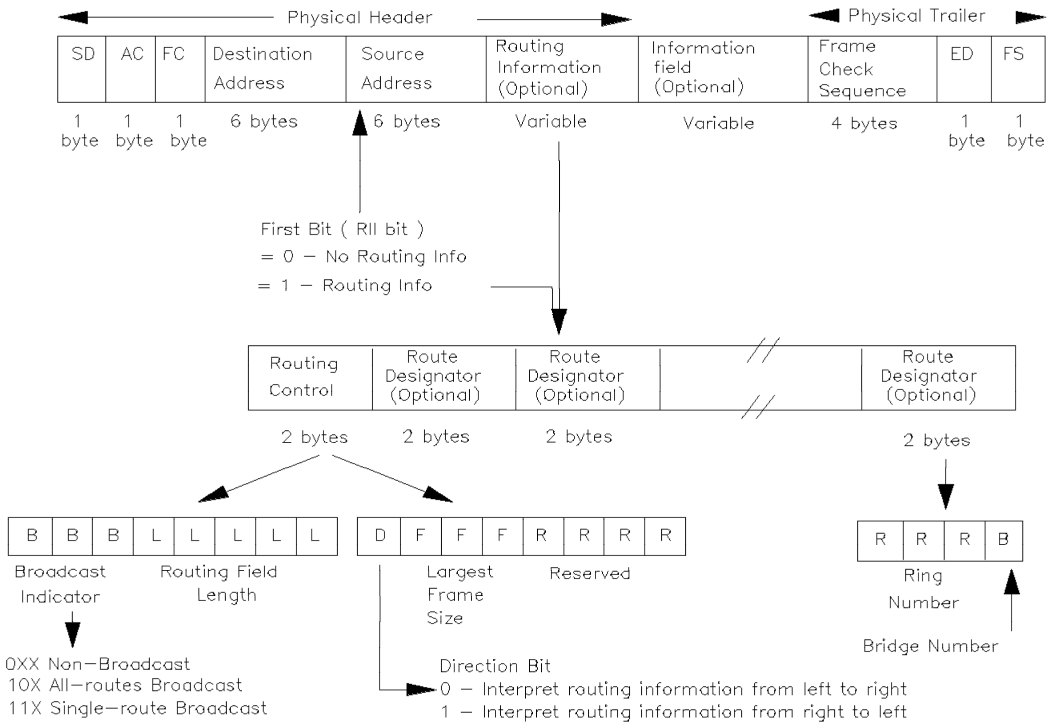
Source routing requires that the originating station provides the routing information. This means that when one station wishes to send data to another station, the sending station must first obtain a route to the destination MAC address.

Route determination is *usually* a two-stage process:

- Stage 1: On-segment route determination
- Stage 2: Off-segment route determination

The term *usually* is used here because, there is no formal method in IBM Token-Ring LANs for route determination. However, the on-segment/off-segment approach described here is relatively common.

In the first stage:



SD	Starting Delimiter
AC	Access Control
FC	Frame Control
ED	Ending Delimiter
FS	Frame Status

Figure 30. Routing Information of a Token-Ring Frame

- The source station sends a frame, usually a TEST or XID LLC Protocol Data Unit (LPDU) onto the local LAN segment[1]. This frame either has no Routing Information Field (RII=0) or it is a non-broadcast frame with RII=1 but without any Route Designator field (RIF=X′0207′). In either case the frame is not forwarded by any of the bridges attached to this LAN.
- The sending station then waits for some time (the time varies depending on the application) and if it does not obtain a response it goes to the second stage of route determination.

For the second stage:

- The sending station resends the TEST or XID LPDU, this time with a stub routing information field with the broadcast bits set. This broadcast may either be an **all-routes** broadcast or a **single-route** broadcast. An example of all-routes broadcast flow is shown in Figure 31 on page 61 and an example of single-route broadcast is shown in Figure 32 on page 62.

[1] This frame is usually sent to SAP 0, a null SAP which is opened automatically by all the adapters and is used to respond to connectionless TEST/XID requests.

- If no response is received from the target station within an a period defined by application, it is the application′s responsibility to retry (stage one and/or two) or backout.

3.5.1.1 All-Routes Broadcast Route Determination

Figure 31 on page 61 is an example of a typical route determination scheme using all-routes broadcast frames. After receiving no responses from the on-segment route determination, the sending station issues an all-routes broadcast TEST or XID frame. All the bridges forward this frame unless:

1. The frame has already been on the next segment.
2. Forwarding the frame would exceed the bridge′s all-route broadcast hop count limit in that direction. IBM limits the number of bridges in a path to seven. Furthermore, each bridge allows the user to further limit how far a frame may travel in a network by setting a hop count limit for that bridge.
3. The bridge filter functions do not allow the frame to be forwarded.

The RIF is built up as the frame crosses the bridges:

- The sending station provides the stub routing control field.
- The first bridge adds two Route Designator fields; the first is the starting ring/bridge combination, and the second is the second segment number and a null bridge entry.
- Successive bridges then fill in their bridge number and add another two-byte Route Designator field containing the next segment number and a null bridge entry.

The routing information of the frame being forwarded through bridge A and bridge D in the example shown in Figure 31, would build up as follows:

After bridge A, the route designators would be 001A 0020
After bridge D, the route designators would be 001A 002D 0030

As many frames as there are routes will be received by the target machine. The target machine responds with a non-broadcast frame, for each received frame, flipping the direction bit in the RIF. The response frames then trace back through the network and arrive at the sending station. Usually the route chosen is the route contained in the first reply, although criteria such as the minimum number of hops the supported frame sizes would be equally valid.

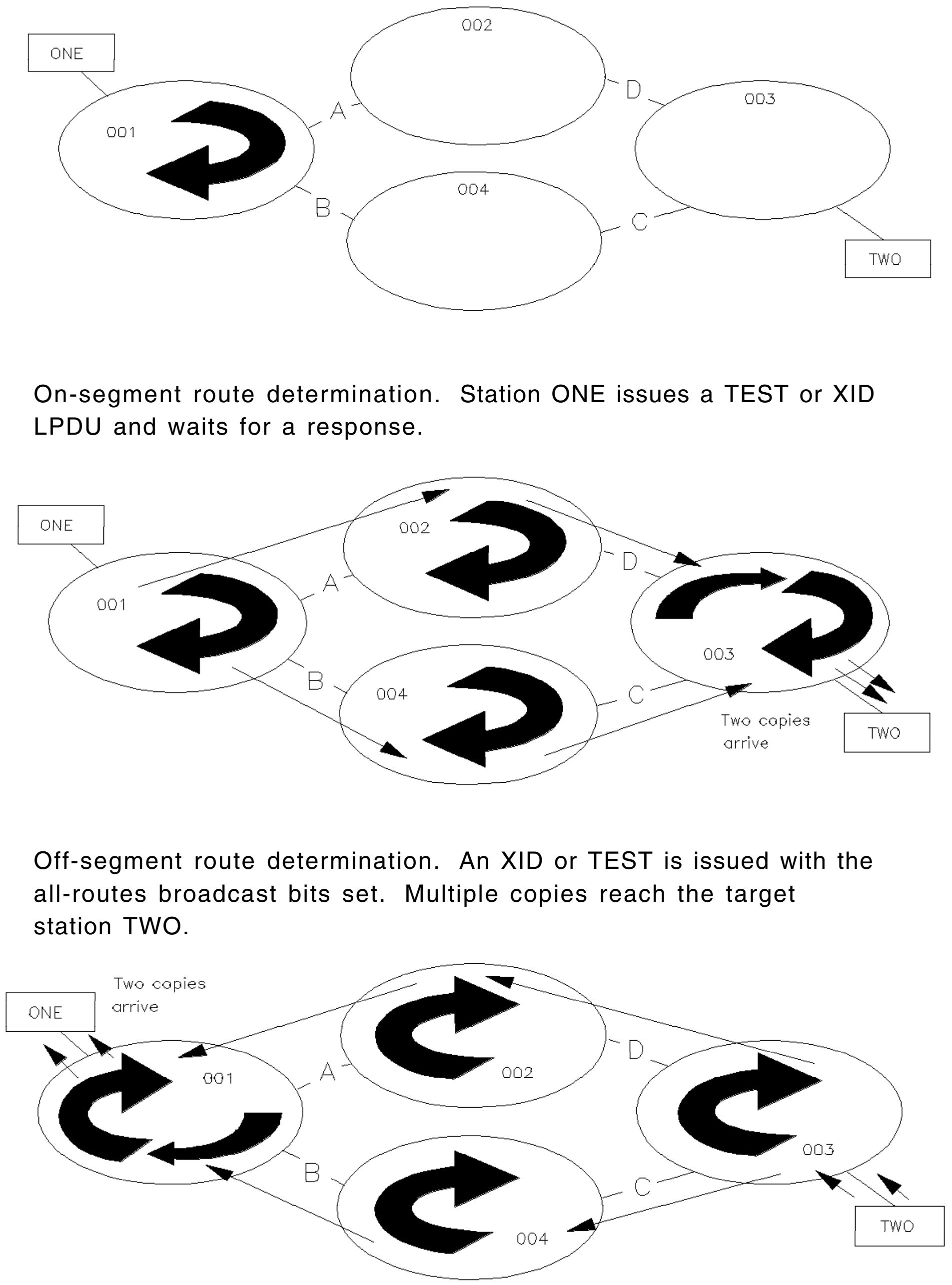
3.5.1.2 Single-Route Broadcast Route Determination

Some products implement single-route broadcast route determination for the second stage of route determination. The sending station resends an XID or TEST LPDU[2], with a stub Routing Information Field. It also sets the single-route broadcast fields in the Routing Control field.

The primary aim of the single-route broadcast function of the IBM Token-Ring Network is to minimize the processing overhead of the target machine (or machines) by only allowing one copy of the broadcast frame on each segment in the LAN. As a result, the target station will receive a single frame.

Note that an all-routes broadcast would cause as many frames as there are possible routes to arrive at the target machine.

[2] Generally to the null SAP, SAP 0.



On-segment route determination. Station ONE issues a TEST or XID LPDU and waits for a response.

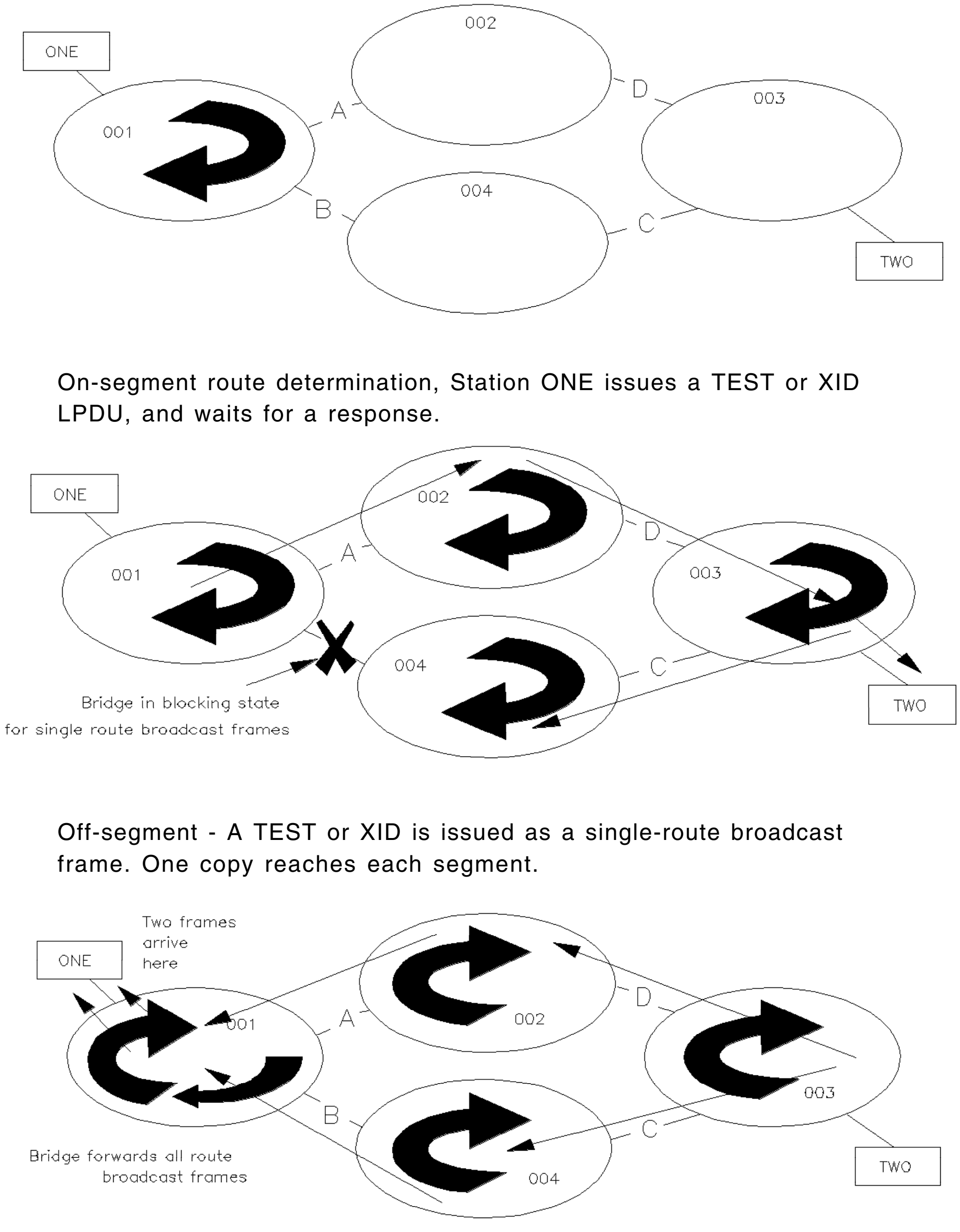
Off-segment route determination. An XID or TEST is issued with the all-routes broadcast bits set. Multiple copies reach the target station TWO.

The target machine responds with non-broadcast frames, that route back to the source. The routing information, when the frames arrive at ONE, is:

1. 001A-002D-0030
2. 001B-004C-0030

With the direction indicator set to 1 - right to left

Figure 31. Example All-Routes Broadcast Route Determination. Station ONE is setting up communication with station TWO.



On-segment route determination, Station ONE issues a TEST or XID LPDU, and waits for a response.

Off-segment - A TEST or XID is issued as a single-route broadcast frame. One copy reaches each segment.

Receiving station TWO responds to the single frame received with an all-routes broadcast frame. Two copies are received by the sending station. The route information fields contain these routes:

1. 003D-002A-0010
2. 003C-004B-0010

With the direction bit set to 0 (that is, read left to right).

Figure 32. Example Single-Route Broadcast Route Determination. Station ONE is setting up communication with station TWO.

The single-route broadcast function is particularly appropriate to LAN server functions, where the number of search requests is significant and where the processor overhead to service multiple broadcast frames could affect response times.

The propagation of single-route broadcast frames is limited by:

- Whether a bridge has been configured to forward single-route broadcast frames.
- Whether the frame has already been on the next segment, as noted in the Route Designator fields built by the previous bridges which the frame has already passed through.
- Filters at the bridge.

The single route is derived from one of the following:

1. Static definition resulting from bridge installation parameters. In this case, the user should specify which bridges are in forwarding state and which bridges are in blocking state. Also, it is the user′s responsibility to ensure that there is a single route active between any two stations. Manual intervention is required to change the route.
2. Single route derived dynamically by using the spanning tree algorithm. The spanning tree algorithm for source route bridges is described later in section 3.5.2, “The Spanning Tree in Source Route Bridges” on page 64.

On receipt of the single-route broadcast frame, the destination station usually issues an all-routes broadcast frame, directed at the source address. The original sending station receives as many frames as there are routes in the network, from which it usually chooses the route taken by the first frame it receives, for subsequent communication.

3.5.1.3 Largest Frame Size Supported by a Bridge

In a multisegment LAN, bridges are only capable of handling certain frame sizes. The largest frame size supported by each bridge is implementation dependent, and may differ from the largest frame supported by the end stations and the largest frame supported by the other bridges. Source routing provides a mechanism whereby the end stations can learn the maximum frame size supported by all the bridges in a route.

The Routing Control field contains an entry for the maximum frame size allowed. This field is initially set by the originator of the broadcast frame to B‘111’. During the forwarding process, each bridge examines this value. If it is higher than that supported by that particular bridge, the bridge lowers the value in the field to the maximum it can support. As broadcast frames are forwarded across the bridges in a path, the maximum frame size allowed for the particular route is obtained. Table 7 shows the allowed frame length values[3].

Table 7 (Page 1 of 2). Maximum Frame Sizes in the Routing Control Field

Largest Frame field	**Size (Bytes)**	**Comments**
B‘000’	516	Minimum for 802.2 LLC Type 1 (connectionless) operation
B‘001’	1500	Largest frame size supported by 802.3 LANs

[3] Many applications and devices do take this field into account and adjust the frame sizes they use accordingly. These applications and devices include OS/2* EE, ES/2, CM/2, Personal Communications/3270, 3174 and 3745.

Table 7 (Page 2 of 2). Maximum Frame Sizes in the Routing Control Field

Largest Frame field	Size (Bytes)	Comments
B'010'	2052	Typical 24x80 full screen application
B'011'	4472	Largest frame size supported by FDDI
B'100'	8144	Largest frame size supported by 802.4 LANs
B'101'	11,407	
B'110'	17,800	
B'111'		Used by all-routes broadcast frames

3.5.2 The Spanning Tree in Source Route Bridges

IBM source route bridges use the spanning tree algorithm to determine the route which will be taken by the *single-route broadcast* frames through a multisegment token-ring LAN.

The spanning tree algorithm used in source route bridges is identical to the spanning tree algorithm used in transparent bridging with the following exceptions:

1. The Hello BPDU is sent to the bridge functional address X′C000000100′.
2. Port ID for a source routing bridge consists of a *ring identifier* and *bridge number* while the Port ID for transparent bridge consists of a *port priority* and *port number*.
3. The spanning tree in source route bridges is used only by the single-route broadcast frames. This means that bridges which are in blocking state will only block the single-route broadcast frames, while they will forward all-route broadcast frames, as well as the non-broadcast frames which carry the appropriate routing information.

   This means that unlike transparent bridges, Source Route bridges support active parallel paths which can be used for load-balancing across bridges as well as providing backup in case of bridge failures.
4. As there is no learning process in the source-route bridges, they can be in one of the following states:
   - Blocking
   - Listening
   - Forwarding
5. Source route bridges do not support the Topology Change Notification protocol, as it is needed only to update the transparent bridge filtering database.

3.6 Source Route Transparent Bridging

To enable users to employ both source routing and transparent bridging within a network to satisfy their unique requirements, the IEEE standard 802.1d has also defined the Source Route Transparent (SRT) bridging. Some of the reasons for the coexistence of source routing and transparent bridging within the same network are:

- Connecting two networks which have been developed separately and in which one uses source routing while the other uses transparent bridging.
- Requirement to connect both types of networks to a single FDDI network.
- Extending multisegment token-ring support for protocols that do not support source routing.

A bridge with the SRT function performs both, the source route and the transparent bridge function. To do so, the SRT bridge looks at the Routing Information Indicator (RII) in the received frames. If RII=0 the frame will be handled by the Transparent bridging logic while the Source Routing logic will process the frame if RII=1.

Figure 33 shows the operation of an SRT bridge.

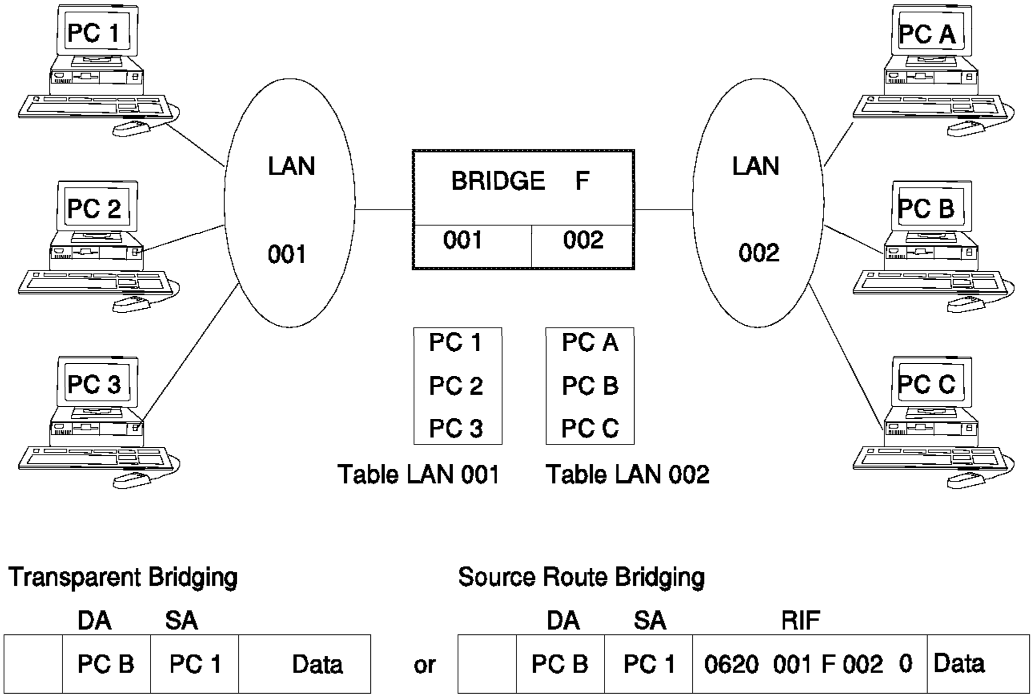


Figure 33. Source Route Transparent Bridging

Although an SRT bridge acts like an SR bridge for the frames with RII=1, there are few differences between SR and SRT as described below:

- Hop count limit

  SR allows a maximum hop count of 7 bridges, while the maximum allowed by SRT is 13. When using SR, the users can set the hop count limit to a value less than the allowed maximum for all-route broadcast frames only, while SRT provides two different settable hop count limits: one for all-route broadcast and one for single-route broadcast frames.

- Largest Frame (LF) size

SR uses 3 bits (bits 1 through 3 in the second byte of the Routing Information Field) for specifying the LF size supported. Table 8 on page 66 shows the LF sizes for SR bridging.

Table 8. LF Size for SR Bridging

Code	LF Size
000	516
001	1500
010	2052
011	4472
100	8144
101	11407
110	17800
111	Used in all-route broadcast only

SRT offers two modes (Base and Extended) for the LF size. The mode used by the bridge is selected by setting an LF mode indicator.

The base mode uses the same 3 bits as the SR, but some of the values are slightly smaller than those defined in the SR.

Extended mode uses 6 bits (bits 1 through 6 in the second byte of the Routing Control field) to specify the LF size.

Table 9 shows the Extended mode LF size for SRT bridging.

Table 9. LF Size for SRT

Base	Extension							
	000	001	010	011	100	101	110	111
000	516	635	754	873	993	1112	1231	1350
001	1470	1542	1615	1688	1761	1833	1906	1979
010	2052	2345	2638	2932	3225	3518	3812	4105
011	4399	4865	5331	5798	6264	6730	7197	7663
100	8130	8539	8949	9358	9768	10178	10587	10997
101	11407	12199	12992	13785	14578	15370	16163	16956
110	17749	20730	23711	26693	29674	32655	35637	38618
111	41600	44591	47583	50575	53567	56559	59551	>59551

3.6.1 SRT and Spanning Tree

When a single network consists of TB, SR and SRT bridges, the following considerations apply to the operation of the spanning tree protocol:

- There are two overlapping spanning trees within the network:

  1. TB and SRT bridges form one spanning tree

  2. SR and SRT bridges form the other

- SRT bridges participate actively in the TB/SRT spanning tree. This means that they issue and process Hello BPDUs addressed to X′800143000000′.

- SRT bridges participate passively in the SR/SRT spanning tree. This means that they forward BPDUs addressed to X′C00000000100′, but they will neither originate nor process these frames.
- The SRT network appears to the SR spanning tree to be a single segment.
- The SR network is invisible to the SRT spanning tree.

3.7 Implications of Using SRT in the Existing SR Networks

In general SRT and SR bridges can coexist in the same network. But there are configurations that could lead to problems. The following topics deal with these problems.

3.7.1 SRT and IBM Token-Ring Bridge

There exists an incompatibility between an SRT bridge and the current version of the IBM Token-Ring Bridge Program or the IBM 8209 TR/TR bridge.

During their internal bridge test, the IBM Bridge Program and IBM 8209 token-ring to token-ring bridge, send a test frame to the MAC address of theirs opposite port with no Routing Information Field (RII=0). This test fails if the frame is received on the opposite port. If there is an SRT bridge in parallel with the IBM Bridge Program or IBM 8209 token-ring to token-ring bridge, it will always forward the bridge test frame resulting in the test failure. Therefore, the IBM Bridge Program and IBM 8209 token-ring to token-ring bridge cannot be in parallel with an SRT bridge. This means that you should not install an SRT bridge in a loop or in parallel with the IBM Bridge Program or the IBM 8209 token-ring to token-ring bridge.

Note that SRT bridges and IBM SR bridges can be installed within the same network in a serial configuration.

3.7.2 SRT and High-Availability Design

The high-availability design for token-ring gateway solutions uses a dual backbone ring and duplicate gateway addresses. An SRT bridge is not recommended between rings on which duplicate addresses appear, because the SRT filtering database associates a bridge port number with an address. This filtering database would be unstable. The value of the port number would depend on which of the duplicate adapters transmitted last.

The recommendations for high-availability design are the following:

- If duplicate addresses are used, make sure there is at least one source route bridge in each path between two adapters. That way, the duplicate address is guaranteed to appear in a transparent bridge frame on at most one port of any SRT bridge in each path. See Figure 34 on page 68 for an example of high-availability design and SRT.

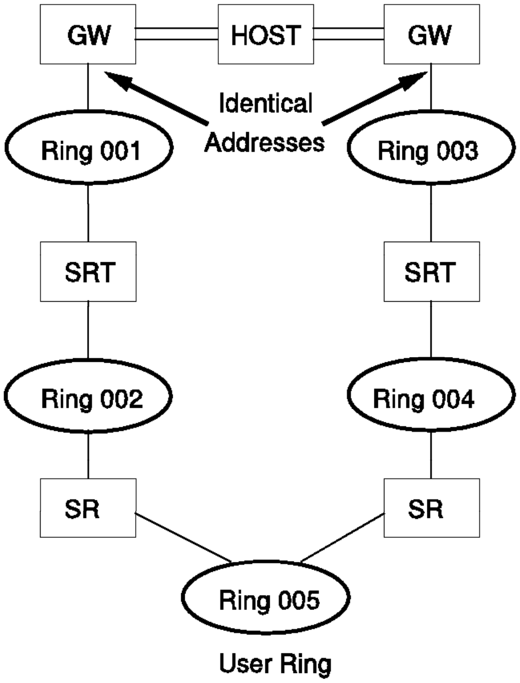


Figure 34. High-Availability Design and SRT

3.7.3 Route Discovery with SRT Bridges

A common method for route discovery used by some programs (for example PCOM/3270) is the following:

- The program sends a local TEST frame that contains no Routing Information Field (RIF) to find its TR gateway.
- An SRT bridge will forward this frame because it does not contain a RIF. This leads to two consequences:
  - The source and the destination station use the spanning tree path of transparent bridging instead of the fastest path of a source routing.
  - Timing problems could occur because the source station thinks that the destination station is on the local ring.

Some Recent products like OS/2 Extended Services (ES) use a different route discovery method that anticipates the possible presence of SRT bridges:

- ES sends a local TEST/XID frame as non-broadcast with no *route descriptors*. This means, the Routing Information Indicator is set to 1 and the RIF contains X′0270′.

  This frame will not be forwarded by the transparent bridging as it contains a RIF. It is not forwarded by source routing either as it does not contain a route.

- If no response, ES sends a single-route broadcast TEST/XID frame with RII set to 1. This frame will be forwarded by the source route bridging.
- If still no response, ES sends a frame without Routing Information (RII=0). This frame will be forwarded by transparent bridging.

Chapter 4. TCP/IP Overview

This chapter is an introduction to the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of communications protocols and applications. We have not attempted to cover in a single chapter what others have published in whole volumes, so you may wish to read other publications on this topic for a more in-depth study.

The following topics are addressed in this overview:

- Architecture
- IP Addressing
- IP Subnets
- IP Routing
- SNMP
- The RFC Process

4.1 The TCP/IP Architectural Model

This section introduces an architectural model for the TCP/IP protocols and deals with some of its basic properties such as internetworking, protocol layering and gateways.

4.1.1 Internetworking

The fundamental design goal of TCP/IP was to facilitate an interconnection of heterogeneous networks and provide universal communication services in such an environment. Each physical network will have its own technology-dependent communication interface, in the form of a programming interface that provides basic communication functions. This concept is known as an **internetwork** or **internet**. There are two main parts to this model.

First, there is the concept of a *universal communication service*. This is provided by a layer (actually multiple layers) of software that fits between the physical network and the user applications and provides a common, universal *interface* for these applications, independent of the underlying physical network. Ultimately, this conceals the underlying network specifics from the end users. TCP/IP applications provide such services according to the protocol definitions upon which they are based. Some commonly known/used TCP/IP services are facilitated via protocols such as those in the following list. There are many others.

- TELNET
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol
- TFTP (Trivial File Transfer Protocol)

The second concept is that of *interconnection*, which makes multiple different physical networks appear as one logical network, (at least from the user′s viewpoint). TCP/IP effects interconnection according to the *Internet Protocol* (IP). The IP allows special nodes known as **gateways** which are attached to multiple physical networks to forward information between them. The IP itself is a significant topic and more information about this protocol and its associated addressing schemes can be found in later sections. Figure 35 on page 72 shows a diagrammatical example of an internetwork or internet.

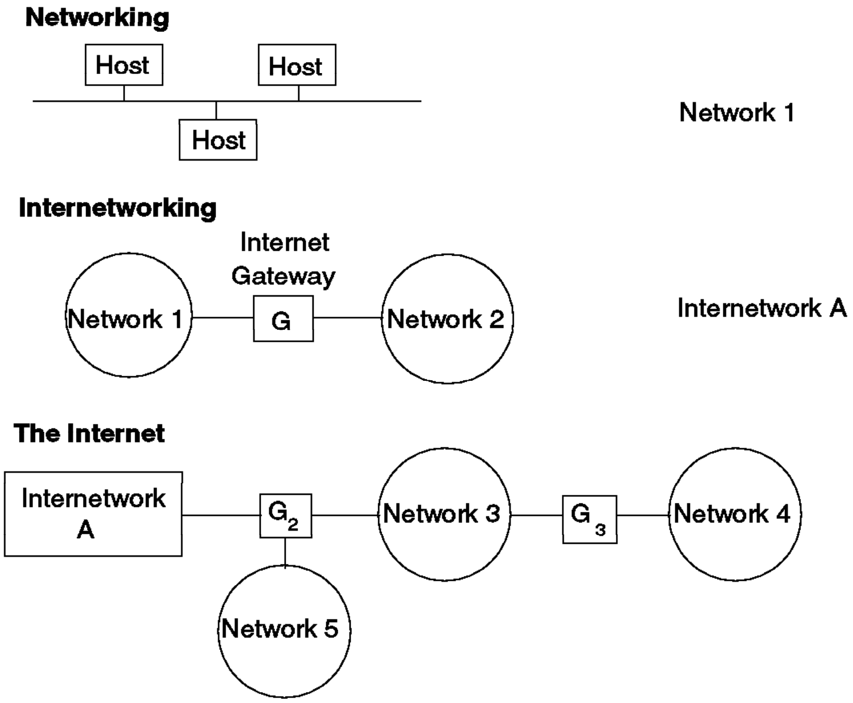


Figure 35. Internetwork or Internet. An interconnected set of networks, seen as one logical network.

Essentially the basic properties of the gateway concept are:

- From the network′s view, a gateway is seen as a normal host.
- From the user′s view, gateways are transparent. The user only sees one large internetwork.

To identify a host on the internetwork, each host is assigned an *IP address* which contains a component to identify the network to which the node belongs and the node itself.

```
IP address = <network address><host address>
```

IP addressing is discussed in detail in 4.2, "IP Addressing" on page 74.

4.1.2 Layered Protocols

The concept of *layering* can be used for situating (but *not* functionally comparing) the TCP/IP protocol suite against others, such as SNA and Open System Interconnection (OSI). Functional comparisons cannot easily be extracted from this, as there are basic differences, even within the *layers* themselves.

The internet protocols can be modeled in the following four functional layers:

Application: at this level we are concerned only with end user software. More specifically, host processes cooperating with other host processes on the same or different networks. Some well known TCP/IP application examples are TELNET (a protocol for remote virtual terminal connections), FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol). Equally applicable at this layer are applications such as AIX NetView/6000 and AIX HMP/6000 which use the services offered by TCP/IP.

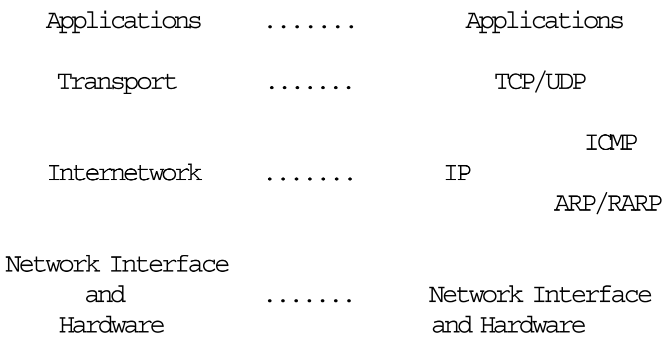
Transport: this is the layer which provides the end-to-end data transfer services. Example protocols at this layer are TCP and UDP (User Datagram Protocol).

A good example of the different services that are provided even within a single layer of the model are TCP and UDP. TCP provides a reliable connection-oriented service whereas UDP provides for the exchange of datagrams without acknowledgments or guaranteed delivery.

Internetwork: this layer provides the *logical* view of the internet (that is, this layer shields the higher layers from the typical network architecture below it). This layer is sometimes referred to as the *IP layer*. The IP protocol is not responsible for reliability, flow control or error recovery, nor does it assume reliability from the lower layers.

Network Interface: this layer is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer.

Figure 36 shows the major inter-layer communications. A more detailed *layering model* is shown in Figure 37 on page 74.



Applications	....	Applications
Transport	....	TCP/UDP
Internetwork	....	IP ICMP ARP/RARP
Network Interface and Hardware	....	Network Interface and Hardware

Figure 36. Architectural Model. Layers represent packagings of functionality.

```
                                        NFS

 Kerb XWin REXEC SMTP TELNET  FTP  DNS TFTP  RPC  NCS SNMP  ..............   Applications

          T  C  P                   U  D  P         .............     Transport

             I  P   and   I  C  M  P                ARP RARP  ....    Internetwork

 Ethernet-IEEE 802.2-X.25-Satellite-Radio-Async-SNA-HYPERchannel ....   ... Network Interface
                                                                             and Hardware
```

Figure 37. Detailed Architectural Model. This model maps TCP/IP services to functional layers.

4.2 IP Addressing

As previously stated, the internet Protocol uses *IP addresses* to uniquely identify nodes on the internet.

IP addresses are 32-bit addresses, usually represented in dotted decimal form. For example:

```
9.67.46.160
```

which is equivalent, in binary, to:

```
0000 1001  0100 0011  0010 1110  1010 0000
```

or in hexadecimal, to:

```
09 43 2E A0
```

There are two logical addresses in each IP address: a *network address*, representing the physical network within the internet, and a *local address*, specifying an individual host or gateway within that network.

```
IP address = <network address><host address>
```

Conceptually, division of the IP address into the network and host components is arbitrary. In practice however, the distribution of addresses to users of the internet must be controlled to preserve uniqueness. The *Network Information Center* (NIC) is responsible for distributing IP addresses.

The NIC assigns the *network* component of the IP address to each organization which wishes to become a member or user of the internet. Each organization itself, is then responsible for ensuring that *host* addresses are unique within their network.

We will investigate how individual organizations may assign addresses in 4.3, “IP Subnets” on page 76, but first let′s look at the IP address structure.

The first few bits of the IP address specify how the rest of the address should be separated into its network and host components. This method has been standardized into three main *classes* of IP addresses.

```
          0 1         8              16             24          31

Class A   0    netID                      hostID


Class B   1 0       netID                         hostID


Class C   1 1 0            netID                          hostID


Class D   1 1 1 0              multicast address
```

Figure 38. Assigned Classes of Internet Addresses

Note that, although the bits used to determine the network class form part of the network address, they cannot be altered within a class. For example, bits 0, 1 and 2 (the three most significant bits) in a class C address are always 1, 1 and 0 respectively. This means that class A addresses will always begin with the range 1-127.x.x.x, class B addresses 128-191.x.x.x, and class C addresses 192-223.x.x.x.

The address classes may be explained as follows:

- **Class A** addresses allocate 7 addressing bits for networks; however addresses of all zeros and all ones are reserved for special purposes (see below for explanation) so this gives us a maximum of 126 unique network addresses (that is 2 to the power 7 less 2). This leaves 24 addressing bits for host addresses. Therefore, a class A address supports a maximum of 16,777,214 (2 to the power 24 less 2) hosts on each of 126 networks.
- **Class B** addresses allocate 14 addressing bits for networks, giving a maximum of 16,382 networks (2 to the power 14 less 2) with 16 addressing bits remaining for hosts resulting in 65,534 (2 to the power of 16 less 2) host addresses on each network.
- **Class C** addresses allocate 21 addressing bits for networks, giving a maximum of 2,097,152 (2 to the power of 21 less 2) network with each network supporting a maximum of 254 (2 to the power of 8 less 2) hosts.
- **Class D** addresses are reserved for multicasting (similar to the broadcasting concept but to a limited network area and only to those hosts with the same class D address). Class D addresses are not as common as the first three.
- There is also a **Class E** address which is denoted by the bit pattern 11110 in the five most significant address bits. The E class is reserved for future use.

It is clear that a class A address will only be assigned to networks with a huge number of hosts, and class C addresses to networks with a small number of hosts.

As stated above, some addresses (both network and host addresses) are reserved for special purposes. Specifically these are:

- **All zeros**

An address of all zeros implies a meaning of **this**. If the IP host address is zero, the meaning is *this host*. If the IP network address is zero, the meaning is *this network*.

It is only meaningful to use such an address where it can be interpreted unambiguously.

For example, when a host wants to communicate over a network, but does not yet know the network IP address, it may send packets with a zero network address. Other hosts on the network will interpret the address as *this network*. Their reply will contain the fully qualified network address which the sender will record for future use.

- **All ones**

  Addresses of all ones are used for **broadcast** transmissions. Broadcast addresses may be specified for networks, hosts or both. An example of a host broadcast address for a class A address is shown below:

  ```
  9.255.255.255
  ```

  This IP address will *broadcast* to all hosts on the 9.0.0.0 class A network.

  This is called a *directed broadcast address* because it contains both a valid (or direct) network address and a broadcast host address.

Although this addressing scheme has proven to be sufficient for more than 10 years, it has one major disadvantage: *if a host moves to another network, its IP address must be changed*.

A second disadvantage is that the addressing scheme, (while it provides a very large number of unique addresses) is finite and one consequence of this is the possibility of IP address space exhaustion. Table 10 lists the network number usage statistics as of April 1992.

Table 10. Internet Usage Statistics

Address Class	Total Addresses	Percentage Used
A	126	38%
B	16382	43%
C	2097152	2%

If the recent trends of exponential growth continue, the network numbers in Class B will soon run out. Although there are only 2% of Class C addresses used, they cannot be used by most networks, because each Class C address can only accommodate up to 254 host addresses.

The solution to this problem is currently the subject of ongoing debates.

4.3 IP Subnets

Due to the explosive growth of the internet, the principle of assigned IP addresses became too inflexible to allow easy changes to local network configurations. Those changes might occur when:

- A new type of physical network is installed at a location.

- Growth of the number of hosts requires splitting the local network into two or more separate networks.
- Increasing distances require splitting a network into smaller networks, with gateways between them.

To avoid having to request additional IP network addresses in these cases, the concept of *subnets* was introduced.

4.3.1 Concept of Subnets

The subnet concept is simply an extension of the IP addressing scheme. However one primary advantage is that the assignment of subnets can be done locally, as the whole network still appears to be one IP network to the outside world.

Standard IP addresses consist of the pair:

<network address><host address>

Subnets are an extension to this by considering a part of the <host address> to be a *local network address* or *subnetwork address*. IP addresses are then interpreted as:

<network address><subnetwork address><host address>

The division of the original <host address> part into a <subnet> and <host> part can be chosen freely by the local administrator. However, once it has been established, it must be used consistently throughout the whole local network.

Assume that our IP network has been assigned the IP network address 129.112.0.0. Now we want to implement multiple physical networks on our site, so we′ll have to make a convention for the <subnet address> part for our whole network. As the given address is a class B address, the local or host component is 16 bits long. We could choose as a subnet convention one the following (non-exhaustive list):

- Bits 0, 1, 8 and 9 are used for the subnet address, that is, the two high order bits of each of the bytes. This gives us 14 possible subnets (16 minus 2, as values 0 and *all ones* have special meanings).
- All even bits are used for the subnet address, the odd ones for the host address. This gives us 254 possible subnets (256 minus 2).
- The first 12 bits are used for the subnet address, the last 4 as host address. This gives us only 14 hosts per subnet.
- The first byte is the subnet address, the second the host address. This gives us 254 possible subnets, each having up to 254 hosts.
- There are many more possible choices.

While you are completely free to assign the subnet part of the local address, it is obvious that assigning a contiguous block of bits at the beginning of the local address part makes the addresses more readable. Let′s take the last possibility in the above list for our example: the first byte specifies the subnet, the second byte specifies the host. Figure 39 on page 78 shows an example of an implementation with three subnets. This convention is formalized in a **subnet mask**. The subnet mask is a 32-bit number, containing binary ones at bit positions corresponding to our subnet bits in the IP address. It is often written in the same format as an IP address. In our example, the subnet mask would be 255.255.255.0.

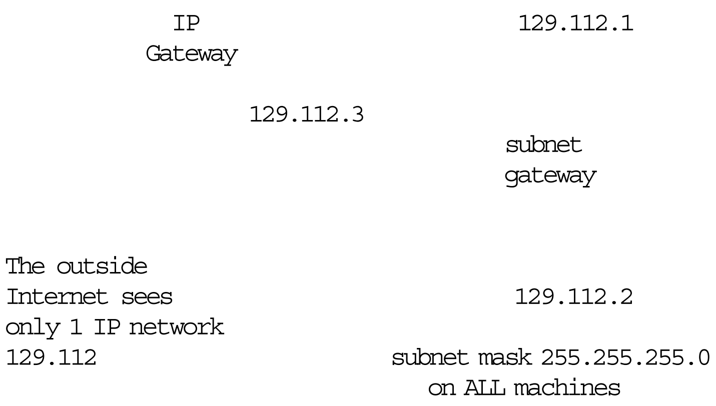


Figure 39. A Subnet Configuration. Three physical networks form one IP network.

Let us now consider a different subnet mask: 255.255.255.240. The fourth octet is then divided in two parts:

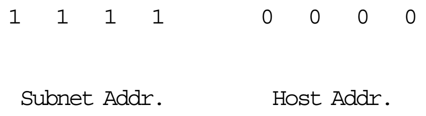


Figure 40. The Fourth Octet of the 255.255.255.240 Subnet Mask

If we assume a class C address, Table 11 contains the valid subnets using this subnet mask:

Table 11 (Page 1 of 2). Subnet Values for Subnet Mask 255.255.255.240

Binary Subnet Address	Decimal Subnet Value
0001	16
0010	32
0011	48
0100	64
0101	80
0110	96
0111	112
1000	128
1001	144
1010	160
1011	176
1100	192

Table 11 (Page 2 of 2). Subnet Values for Subnet Mask 255.255.255.240

Binary Subnet Address	Decimal Subnet Value
1101	208
1110	224

For each of these subnet values, only 14 addresses (from 1 to 14) for hosts are available, because only the right part of the octet can be used and because addresses 0 and 15 (all bits set to one) have a special meaning.

Thus the subnetwork address 9.67.32.16 will contain hosts whose IP addresses are in the range of 9.67.32.17 to 9.67.32.30, and subnetwork address 9.67.32.32 will contain hosts whose IP addresses are in the range of 9.67.32.33 to 9.67.32.46, etc.

4.4 IP Routing

An important function of the IP layer is *IP routing*. It forms the basic mechanism for interconnecting different physical networks, (one of the fundamental capabilities of the internet). In fact, the IP routing mechanism is sufficient to perform basic gateway functions itself. This means that any host on the internet can be at the same time a normal host and a gateway. Routing can in fact be more complex and sophisticated than described here; however, this will suffice as an introduction to the topic.

This *basic* kind of IP gateway is referred to as a *gateway with partial routing information*, because this type of gateway only has information about the hosts directly attached to the physical networks to which this machine is attached. Additional protocols are needed to implement a *full-function* gateway, as used on the internet. These will not be covered here.

4.4.1.1 Direct and Indirect Destinations

If the destination host is attached to a network to which the source host is also attached, an IP datagram can be sent directly, simply by encapsulating the IP datagram in the physical network frame. This is called *direct* delivery and is referred to as *direct routing* by the IP routing algorithm.

Indirect routing occurs when the destination host is not on a network directly attached to the source host. The only way to reach the destination is via one or more IP gateways. The address of the first of these gateways (the *first hop*) is called an *indirect route* in the context of the IP routing algorithm. The address of the first gateway is the only information needed by the source host.

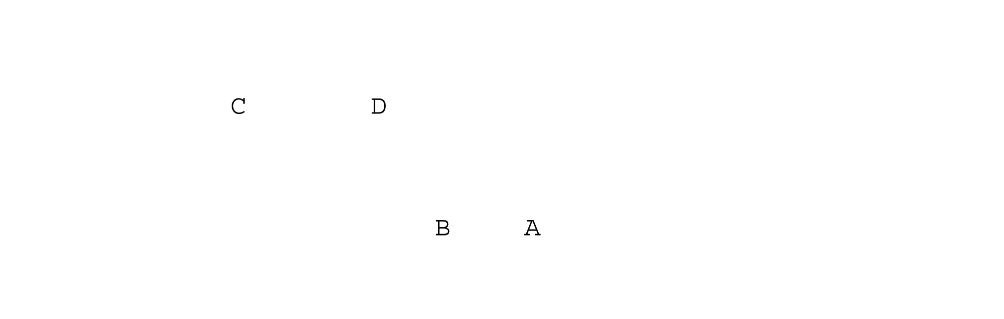


Figure 41. Direct and Indirect IP Routes. Host A has a direct route to hosts B and D, and an indirect route to host C.

The consequence of this is that the only addresses an individual host must know are:

1. Hosts attached to the *direct* networks. This can be determined simply by looking at the IP network address part of the total IP address - it is the same as the IP address of the source machine itself.
2. For *indirect* hosts, the only knowledge required is the IP address of a gateway leading to the destination *IP network*. Again, the only information needed is the IP network address part of the destination address.

The obvious conclusion is that the IP routing mechanism only considers the IP network address part of destination IP addresses.

Some IP implementations will also support explicit host routes, that is, a route to a specific IP address (including local part). These explicit routes are only to be used for exceptional conditions and will not be considered further here.

4.4.1.2 IP Routing Table

Each host keeps the set of mappings between:

- Destination IP network address
- Route to next gateways

in a table called the *IP routing table*.

Three types of mappings can be found in this table:

1. The direct routes, for locally attached networks.
2. The indirect routes, for networks reachable via one or more gateways.
3. The default route, which contains the (direct or indirect) route to be used in case the destination IP network is not found in the mappings of type 1 and 2 above.

See the network in Figure 42 on page 81 for an example configuration.

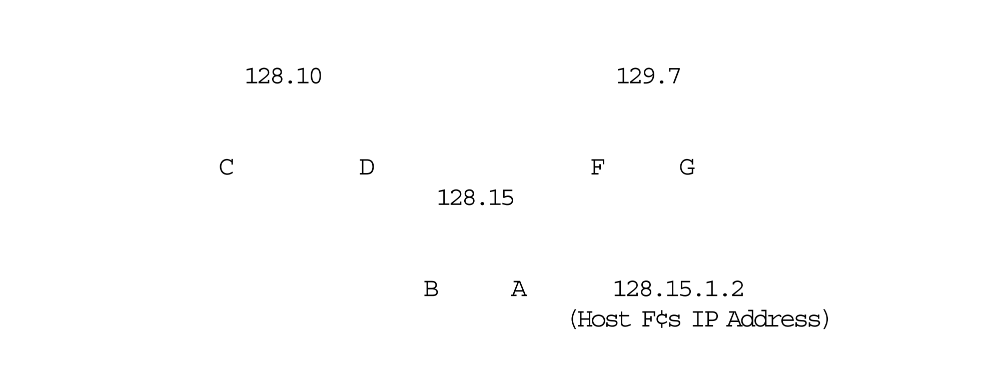


Figure 42. Example IP Routing Table

The routing table of host D will contain the following entries:

Table 12. Host D Routing Table

Destination Network Address	Route
128.10	direct attachment
128.15	direct attachment
129.7	128.15.1.2
default	128.15.1.2

4.4.1.3 IP Routing Algorithm

From the foregoing discussion, one can easily derive the steps that IP must take in order to determine the route for an outgoing datagram. It is called the *IP routing algorithm*:

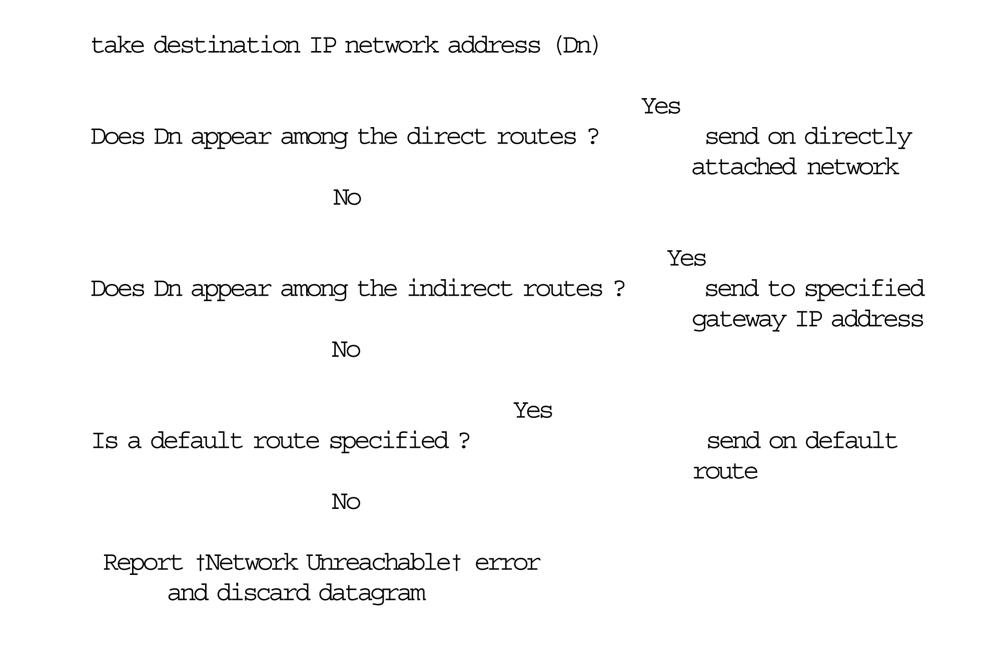

take destination IP network address (Dn)
Yes
Does Dn appear among the direct routes ?
send on directly attached network
No
Yes
Does Dn appear among the indirect routes ?
send to specified gateway IP address
No
Yes
Is a default route specified ?
send on default route
No
Report †Network Unreachable† error and discard datagram

Figure 43. IP Routing Algorithm

Note that this is an iterative process. It is applied by every host handling a datagram, except of course for the host to which the datagram is actually addressed.

4.4.1.4 IP Routing with Subnets

To route an IP datagram on the network, the general IP routing algorithm has the following form:

```
     destination IP network address = my IP network address ?

          yes                          no

    send IP datagram             send IP datagram
    on local network             to gateway corresponding
                                 to the destination IP
                                 network address
```

Figure 44. IP Routing without Subnets

To differentiate between the subnets, the IP routing algorithm is changed to:

```
     bitwise_AND(destination IP address,subnet mask)
                           =
         bitwise_AND(my IP address,subnet mask)    ?

          yes                          no

    send IP datagram             send IP datagram
    on local network             to gateway corresponding
                                 to the destination IP
                                 (sub)network address
```

Figure 45. IP Routing with Subnets

Some major implications of this new algorithm are:

- This algorithm is a change to the *old* IP algorithm. Therefore, to be able to operate this way, the particular gateway must contain the new algorithm. Some implementations may still use the *old* algorithm, and will not function in a *subnetted* network.
- As IP routing is used on *all* of the machines (not only the gateways), *all* of the machines on the subnet must:
  1. Have an IP algorithm that supports subnetting.
  2. Have the same subnet mask (unless subnets are formed within the subnet).
- If the IP on any of the machines does not support subnetting, this machine will be able to communicate with any host on its own physical network, but will not communicate with any machine on another physical network within the same *subnetted* IP network because this host sees only one IP network and its routing cannot differentiate between an IP datagram directed to a

host on the local network and a datagram that should be sent to a *subnet* gateway.

4.5 SNMP

The basic implementation of SNMP defines the **Network Management Station** as the network node that executes the network management applications (such as AIX NetView/6000) to monitor and control **Network Elements** such as hosts and gateways.

Essentially, the network management station (SNMP manager) issues management requests to a network element′s **SNMP Agent**. Agent software executes the requested task and returns the result to the network management station. Communication between the network management station and the agent is facilitated via the SNMP.

By definition and design, SNMP explicitly minimizes the complexity of management functions available to the SNMP agent. Table 13 describes the commands or verbs that the network manager may issue to the agent and, in the case of the **trap**, from the agent to the network manager:

Table 13. SNMP Verb Descriptions

Verb	Description
get	Requests the SNMP agent on the managed network element to retrieve the value of a particular variable and return it to the requesting network management station.
set	Requests the SNMP agent to update a variable on the managed network element and by implication change the system value that it represents.
get next	Requests the SNMP agent on the managed network element to progress to the next variable after the one specified in the request and return it to the requesting network management station. This provides a powerful way for the network management station to *learn* the configuration of a remote system.
trap	Sends an unsolicited message to the management station describing an extraordinary event. The *trap* mechanism provides a useful means of initiating the flow of management information from the SNMP agent.

In general, a network management station keeps itself up-to-date on the status and configuration of the network by regularly polling each of the nodes in its management domain. Obviously we need to balance the network load attributable to management polling with the need to gather information. Depending on the number of nodes in the network, a significant time lapse may occur between polls. However, there are undoubtedly occasions when it is beneficial or indeed necessary for the agent to inform the network manager of an extraordinary event which cannot wait until the next scheduled poll. As we learned in Table 13, the *trap* is the mechanism which provides this facility.

For example, when a node comes online it may take a long time for the management station to discover it. This process is hastened if the new node′s agent sends a *cold-start* trap to the network manager.

The trap is a simple structure comprising one of six generic types, some optional specific information, the IP address of the originating agent and a reference to the affected system component. The intention is that the trap is a trigger, to inform the management station of an extraordinary event. To fill in the details, the management station is then expected to poll the agent using SNMP *get* and *get next* commands.

4.5.1 Abstract Syntax Notation

Because we are dealing with a heterogeneous environment, the variables used to represent the resources on the managed network element need to be encoded in a platform independent way. This is effected by using a subset of the OSI data description language called **Abstract Syntax Notation One**, (ASN.1). ASN.1 is a formal language of considerable complexity and it is neither useful nor necessary to describe it here.

SNMP employs only a subset of ASN.1 in order to enforce consistency with its definition. This is known as **Structure and Identification of Management Information** (SMI).

Objects defined using ASN.1 (and by implication SMI) are organized in a classic *inverted tree* format, where each level of the tree provides a more detailed description. Such a tree is termed an **Object Identifier Tree**.

At each level of the identifier tree the branches are numbered so that any object may be uniquely identified by a sequence of digits.

For example, the branches leading to what is known as the standard internet **Management Information Base** (MIB) are shown in Figure 46 on page 85. Thus, all standard internet MIB objects have a dotted decimal notation which commences with:

```
.1.3.6.1.2.1...
```

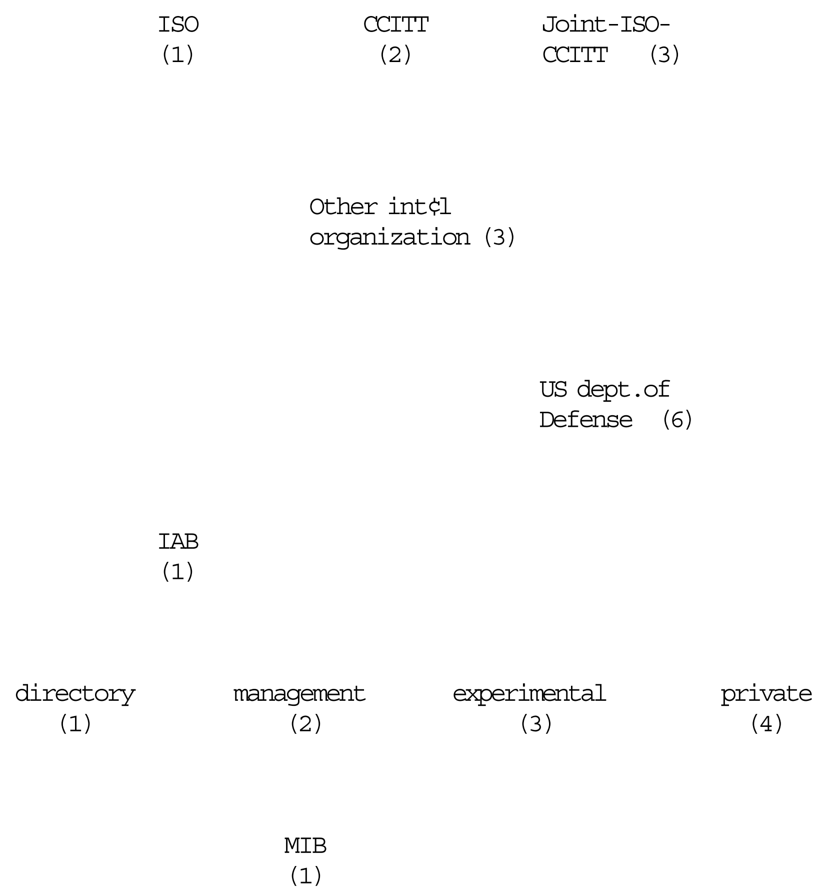


Figure 46. ISO Object Identifier Tree for TCP/IP-Based Networks

Note that the initial period denotes the *root* of the tree.

4.5.2 The Management Information Base (MIB)

In the example above, we have used the notation of the standard internet MIB. This MIB defines the standard set of objects that all SNMP agents must support in order to comply with the definition. There are in fact two definitions which are commonly known as MIB-I and MIB-II. MIB-I contains 114 objects which have been augmented to 171 to form MIB-II.

The standard internet MIB is divided into the following eight groups:

1. **System:** Describes the environment and capabilities of the agent.
2. **Interfaces:** Contains details of the physical network interfaces.
3. **Address Translation:** Contains information about mappings between physical and internet addressing schemes.
4. **IP:** Contains details of the activity and capabilities of the internet protocol on the agent.
5. **ICMP:** Statistics about the internet control message protocol traffic.

6. **TCP:** Statistics and capabilities of the transmission control protocol on the agent.
7. **UDP:** Statistics about user datagram protocol activity on the agent.
8. **EGP** Statistics configuration information about the external gateway protocol functions on the agent.

The management information base is not, as the name suggests, a database in the sense of a physical collection of data. The object variable instances defined within the MIB are maintained by many different system functions and specific information is only brought into SNMP agent storage when an explicit request for it is received from the network management station.

4.5.2.1 MIB Extensions

The internet standard MIB represents the lowest common denominator of TCP/IP related information. The SNMP and ASN.1 do not impose any restrictions on extending the information base. In fact the SNMP was defined with this purpose in mind.

Many suppliers provide MIB extensions with their products to enhance the functional management of their equipment in an SNMP environment. The *ibm-8250.mib* MIB that is supplied with AIX HMP/6000 for the IBM 8250 Multiprotocol Intelligent Hub is a good example.

Extensions to the MIB should be located off the *experimental* and *private* branches depending on their intended use. For commercial concerns there is an *enterprises* branch (branch (1)) off the *private* branch. Sub-branches off this are allocated to individual enterprises. IBM has been allocated number 2, so all IBM *enterprise specific* MIB objects have a dotted decimal notation commencing with .1.3.6.1.4.1.2. The structure showing the IBM enterprise MIB is shown in Figure 47 on page 87.

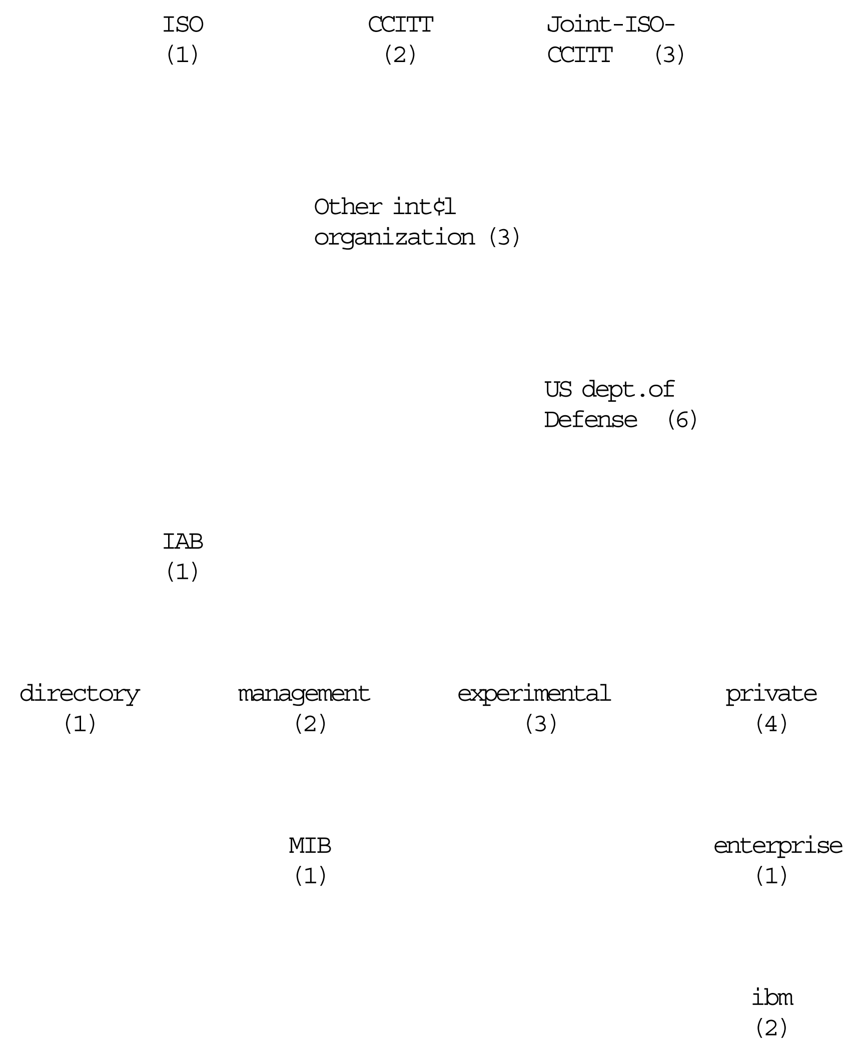


Figure 47. ISO Object Identifier Tree for TCP/IP-Based Networks, Extending the MIB

The only requirement placed on objects added in this way is that they use correct ASN.1 notation within the limits of the SMI definition.

AIX NetView/6000 provides support for several MIB extensions from IBM and other manufacturers, and is dynamically extendable to support any valid definition.

4.5.3 Adding Agent Management Function

Clearly there is no point in adding object definitions to the MIB if it is not also possible to add management applications to bind those definitions to real resources. Many SNMP implementations provide a protocol to allow user written applications to register and manage private MIB extensions. These applications are termed **subagents**.

Usage of a subagent protocol is transparent to the SNMP manager. It is the SNMP agent′s responsibility to translate the requests to the subagent protocol and to forward them to the subagent itself.

4.5.4 The Community Name

SNMP **community** names are used to control access to the MIB values of an agent. The AIX */etc/community* file associates a community name with an agent host name. SNMP applications such as AIX NetView/6000 and AIX HMP/6000 use this file to determine which SNMP community name to use for SNMP requests to specific agents.

A community name must be configured for both the agent and the manager. If an SNMP request with an invalid community name is sent to an agent, the agent will generate an *authentication failure* trap.

The community name is associated with all of the agent′s MIB values, not with subsets of the agent′s MIB. Community names are not secure; they are transmitted unencrypted across the network.

Multiple community names may be configured for an agent and may be assigned to multiple network management stations.

AIX NetView/6000 also allows a **view** name to be defined for a community name on an agent. This is used to further control which MIB values are *seen* by the network manager.

Note

As the view is defined by the network management station it is considered a *control* feature rather than a *security* feature.

4.6 The Request For Comment (RFC) Process

The internet protocol suite (which includes everything discussed in this chapter) is continually evolving through a mechanism known as a *Request For Comments* (RFC). New protocols (mostly application protocols) are being designed and implemented by researchers, and are brought to the attention of the internet community in the form of an RFC.

The internet Activity Board (IAB) maintains a list of RFCs that define standards for the internet protocol suite. Each protocol is assigned a *state* and a *status*.

An internet protocol can have one of the following **states**:

- ***Standard***: The IAB has established this as an official protocol for the internet. These are separated in two groups:
  1. IP protocol and above, protocols that apply to the whole internet.
  2. Network-specific protocols, generally specifications of how to do IP on particular types of networks.
- ***Draft standard***: The IAB is actively considering this protocol as a possible standard protocol. Substantial and widespread testing and comments are desired. Comments and test results should be submitted to the IAB. There

is a possibility that changes will be made in a draft protocol before it becomes a standard.

- ***Proposed standard***: These are protocol proposals that may be considered by the IAB for standardization in the future. Implementations and testing by several groups are desirable. Revision of the protocol is likely.
- ***Experimental***: A system should not implement an experimental protocol unless it is participating in the experiment and has coordinated its use of the protocol with the developer of the protocol.
- ***Informational***: Protocols developed by other standard organizations, or vendors, or that are for other reasons outside the purview of the IAB, may be published as RFCs for the convenience of the internet community as informational protocols. Such protocols may in some cases also be recommended for use in the internet by the IAB.
- ***Historic***: These are protocols that are unlikely to ever become standards in the internet either because they have been superseded by later developments or due to lack of interest.

Definitions of Protocol **status**:

- ***Required*** *protocol*: A system must implement the required protocols.
- ***Recommended*** *protocol*: A system should implement the recommended protocol.
- ***Elective*** *protocol*: A system may or may not implement an elective protocol. The general notion is that if you are going to do something like this, you must do exactly this.
- ***Limited use*** *protocol*: These protocols are for use in limited circumstances. This may be because of their experimental state, specialized nature, limited functionality, or historic state.
- ***Not recommended*** *protocol*: These protocols are not recommended for general use. This may be because of their limited functionality, specialized nature, or experimental or historic state.

All RFCs are available publicly, both in printed and electronic form from the Network Information Center (NIC). References to the RFCs will be made throughout this document, since they form the basis of all TCP/IP protocol implementations.

- They can be obtained in printed form from:

  Government Systems, Inc.
  Attn: Network Information Center
  14200 Park Meadow Drive
  Suite 200
  Chantilly, VA 22021
  USA

  Help Desk Telephone Numbers:
  1-800-365-3642 (1-800-365-DNIC)
  1-703-802-4535
  Fax Number: 1-703-802-8376

  Help Desk Hours of Operation:
  7:00 am to 7:00 pm Eastern Time

Network Address: 192.112.36.5 (NIC.DDN.MIL)

Root Domain Server: 192.112.36.4 (NS.NIC.DDN.MIL)

- To get the electronic form, users may use an *anonymous* FTP to the host NIC.DDN.MIL and retrieve files from the directory *rfc*.
- RFCs can also be obtained through the IBM VNET network using the following command:

```
¢EXEC TOOLS SENDTO ALMVMA ARCNET RFC GET RFCnnnn TXT *¢
```

Where *nnnn* refers to the number of the RFC.

To obtain a list of all the RFCs (and to know if they are available in TXT format or in PostScript format), use the command:

```
¢EXEC TOOLS SENDTO ALMVMA ARCNET RFC GET RFCINDEX TXT *¢
```

To give an idea of the importance of the major protocols, we list some of them together with their current state and status:

Table 14 (Page 1 of 2). Some Internet Protocols and Their Current State and Status

Protocol	**State**	**Status**
Internet Protocol (IP)	Standard	Required
Internet Control Message Protocol (ICMP)	Standard	Required
Address Resolution Protocol (ARP)	Standard	Elective
Reverse Address Resolution Protocol (RARP)	Standard	Elective
Transmission Control Protocol (TCP)	Standard	Recommended
User Datagram Protocol (UDP)	Standard	Recommended
Structure of Management Information (SMI)	Standard	Recommended
Management Information Base (MIB-I)	Historic	Not Recommended
Management Information Base-II (MIB-II)	Standard	Recommended
Simple Network Management Protocol (SNMP)	Standard	Recommended
Border Gateway Protocol 3 (BGP3)	Draft Standard	Elective
Routing Information Protocol (RIP)	Standard	Elective
Open Shortest Path First Protocol V2 (OSPF2)	Draft Standard	Elective
OSI IS-IS for TCP/IP Dual Environments (IS-IS)	Proposed Standard	Elective
Gateway to Gateway Protocol (GGP)	Historic	Not Recommended
TELNET Protocol (TELNET)	Standard	Recommended
File Transfer Protocol (FTP)	Standard	Recommended
Simple Mail Transfer Protocol (SMTP)	Standard	Recommended
Domain Name System (DOMAIN)	Standard	Recommended

Table 14 (Page 2 of 2). Some Internet Protocols and Their Current State and Status

Protocol	**State**	**Status**
Bootstrap Protocol (BOOTP)	Draft Standard	Recommended
Network File System Protocol (SUN-NFS)	Proposed Standard	Elective
Remote Procedure Call Protocol (SUN-RPC)	Proposed Standard	Elective
Trivial File Transfer Protocol (TFTP)	Standard	Elective
NetBIOS Services Protocol (NETBIOS)	Standard	Elective

A complete list of the state and status of protocols can be found in *IAB Official Protocol Standards*. The IAB intends to issue an update to this memo approximately quarterly. The current update is described in RFC 1360 (September 1992).

Chapter 5. AIX NetView/6000 Overview

This is an overview of AIX NetView/6000 Version 1.1 which at the time of writing was the latest version of the software to support AIX HMP/6000. All the information provided in this book applies to and has only been tested on this level of the software.

This chapter will cover the following topics:

- The AIX NetView/6000 product
- The features of AIX NetView/6000
- The components of AIX NetView/6000
- Sources of additional information

5.1 The Product

AIX NetView/6000 is an IBM application program which allows network administrators to use SNMP to manage distributed and heterogeneous networks from an IBM RISC System/6000* running AIX Version 3.2. It also monitors IP addressable devices that are not running SNMP agents by using Internet Control Message Protocol (ICMP) echo requests. It includes several network management applications, including fault monitoring and diagnosis, performance monitoring and network configuration applications. It also has tools to help you build your own management related applications and integrate them into AIX NetView/6000.

AIX NetView/6000 provides an easy to use graphical user interface, based on OSF/Motif, that provides a dynamic graphical topology map and access to network management applications and diagnostics facilities.

AIX NetView/6000 also integrates with IBM′s host NetView product via the AIX NetView Service Point application. This allows AIX NetView/6000 to convert AIX *traps* to SNA *alerts* and to forward them to host NetView for monitoring.

Although AIX NetView/6000 is a very functional application in its own right, one of its key strengths lies in its design which allows other SNMP-based applications to use the services it provides. AIX HMP/6000 is a good example of an application which uses the AIX NetView/6000 autodiscovery, trap monitoring, and community and trap configuration files.

5.2 AIX NetView/6000 Features

AIX NetView/6000 provides the following features:

- Dynamic discovery of the network topology, including IP hosts, gateways and networks.
- The ability to specify a management region that limits or extends the scope of network elements that are dynamically discovered.
- A multi-level graphical representation of the network topology of an IP-based internet, including an internet level, a network level and a segment level.

- Automatic layout of the network topology to eliminate the need to manually structure the nodes on the topology map.
- Dynamic map automatically updates whenever status, topology or configuration changes occur in the network.
- Editing operations to modify the topology map to represent information that cannot be dynamically discovered.
- Point and click selection model to perform network management operations on specific objects.
- Operations for quickly locating objects by various attributes.
- Map snapshots for saving past network configurations and for network planning.
- Tools for diagnosing network problems and testing network connectivity, finding routes, and requesting network information from remote nodes.
- Access to remotely managed nodes and remote system administration applications to resolve identified network problems.
- Configuration of events provides a way to automatically invoke a customized action on receipt of a specific event.
- User-configurable thresholds that use the data collector and thresholds operation.
- Graphical problem diagnostics.
- Detailed notification of problems on the network.
- Display of events and SNMP traps by category or selected node.
- Tools for accessing both standard and enterprise specific MIBs, building MIB applications and collecting MIB information.
- Network performance information in a line graph form showing statistical trends.
- User-configurable polling intervals to regulate the amount of network traffic generated by the network management station.
- Bidirectional communication between NetView and AIX NetView/6000 via AIX NetView Service Point, enabling shared network management in a combined Systems Network Architecture (SNA) and TCP/IP environment.
- Reconfiguration of the network management application itself to support extensions provided by the remote agents.
- Conversion of AIX alertable errors to traps by a subagent and forwarding to AIX NetView/6000 to send to NetView as SNA alerts.
- Online indexed help system that provides detailed information about AIX NetView/6000.
- Online product documentation, including comprehensive administration and reference information.

5.3 Components of AIX NetView/6000

The components of AIX NetView/6000 include the following items. Note that an AIX **daemon** is an AIX process that is being run in the *background*. This simply means that the process is hidden from the user, except where the output is specifically meant for the user.

- The **trapd** daemon

  The */usr/bin/trapd* daemon receives traps, forwards them to all connected daemons and logs events. The trapd daemon logs all events to a file; the default file is /usr/adm/trapd.log. This ASCII file serves as both the network event log and log file for trapd and netmon errors. This daemon must always be running for the xnm application to execute.

- The **netmon** daemon

  The */usr/bin/netmon* daemon polls agents initially to discover the network topology and then to detect topology, configuration and status changes in the network. Netmon uses ICMP echo requests (ping) to poll nodes for status and SNMP commands to poll nodes for MIB values. Based on the discovered information, netmon generates the topology map.

  The polled values retrieved by netmon are stored in a set of files called the *topology database*, /usr/etc/nm/databases/topo_db. If the database does not initially exist, netmon will create it during discovery of the network and generation of the map. Once the topology database is generated, the xnm application reads it at startup to receive information about redrawing the topology map on the user interface.

- The **tralertd** daemon

  The */usr/bin/tralertd* daemon is used in an environment where both SNA and TCP/IP protocols are running. Tralertd receives events and traps from trapd. If a trap has been configured to be converted to an SNA alert, tralertd is responsible for effecting this. The tralertd daemon then sends the SNA alert to NetView via AIX NetView Service Point.

- The **spappld** daemon

  The */usr/bin/spappld* daemon provides a command interface for NetView to AIX NetView/6000 in an environment running SNA and TCP/IP protocols. Spappld receives and executes NetView RUNCMDs in the internet environment, and sends the responses to NetView via AIX NetView Service Point.

- The **snmpd** daemon

  The */usr/bin/snmpd* daemon is included as part of the AIX Version 3.2 operating system. This daemon provides the SNMP agent with processes for the management of AIX network nodes.

- The **trapgend** daemon

  The */usr/bin/trapgend* daemon is a subagent provided with AIX NetView/6000 that converts AIX alertable errors to SNMP traps.

  On AIX Version 3.2 systems, system errors are logged by the AIX error logging facilities in the /dev/error special file. AIX NetView/6000 installs an entry in the AIX *Object Data Manager (ODM)* which directs the AIX error logging daemon, *errdemon*, to notify the trap process when alertable errors are logged. These alertable errors are forwarded by the trap process to the trapgend daemon, which converts them into SNMP traps. Using what is termed the SMUX protocol, trapgend forwards the traps it generates to the trapd daemon on the AIX NetView manager specified by the trap destination.

Trapgend also provides a trap throttle to suppress identical trap generation, allows remote ping operations from AIX NetView/6000 and supports CPU utilization and disk space monitoring MIB extensions.

- The **snmpCollect** daemon

  The */usr/bin/snmpCollect* daemon collects, compares and stores SNMP agent MIB values. It also checks the collected values against user-defined thresholds and generates events if the thresholds are exceeded.

- The **xnm** application

  The */usr/bin/X11/xnm* application is the principal user interface for AIX NetView/6000. The xnm application is based on OSF/Motif user interface guidelines. The application may be started by executing either /usr/bin/nv6000 or /usr/bin/X11/xnm. If you are the root user the /usr/bin/nv6000 shell script will start all the AIX NetView/6000 daemons as well as xnm. If you are not the root user, the script only starts the xnm application. /usr/bin/X11/xnm starts only the xnm application. If the trapd daemon is not running, the xnm application will not start.

- The **xnmevents** process

  The */usr/etc/nm/bin/eui/xnmevents* process is automatically invoked by the xnm application and displays pending events in the main window Control Desk in either the Event Cards or List presentation format. The xnmevents process reads the */usr/etc/nm/tmp/xnmevents.save* file at system startup to recover previously unacknowledged events and the events′ last exit date and time. This process also reads the *trapd.log file* at startup to determine which events in the file occurred since the process was last running. The xnmevents.save file does not include those events from the trapd.log file that are defined to be logged only.

- The **xnmappmon** process

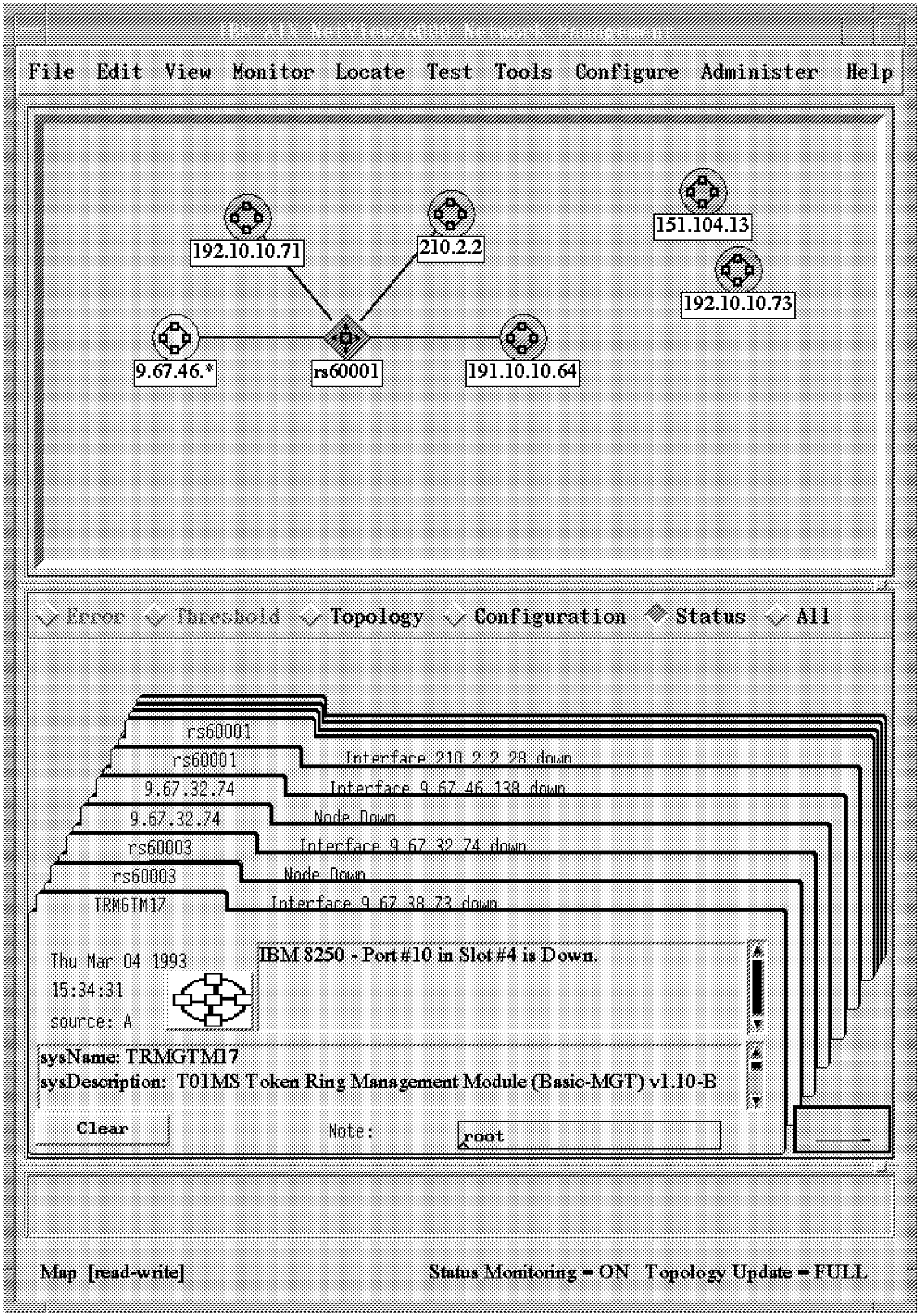
  The */usr/etc/nm/bin/xnmappmon* process is also invoked by the xnm application. It manages the dialog boxes for management operations that have text output and are non-interactive.

- The **xstatmon** application

  The */usr/etc/nm/bin/xstatmon* application graphs a set of monitored statistics and is started by the xnm application when it is needed.

5.3.1.1 A Brief View - xnm

AIX NetView/6000 provides two primary interface windows. The AIX NetView/6000 **console** window, shown in Figure 48 on page 97, is the main interface and is displayed automatically when *xnm* is invoked. It provides access to all the AIX NetView/6000 functions plus other user built applications, the AIX SMIT tool, and AIX HMP/6000 if it is installed.



rs60001

rs60001 Interface 210.2.2.28 down

9.67.32.74 Interface 9.67.46.138 down

9.67.32.74 Node Down

rs60003 Interface 9.67.32.74 down

rs60003 Node Down

TRMGTM17 Interface 9.67.38.73 down

Thu Mar 04 1993
15:34:31
source: A

IBM 8250 - Port #10 in Slot #4 is Down.

sysName: TRMGTM17
sysDescription: T01MS Token Ring Management Module (Basic-MGT) v1.10-B

Note: root

Map [read-write]   Status Monitoring = ON Topology Update = FULL

Figure 48. The AIX NetView/6000 Console Window. This is the main AIX NetView/6000 interface window.

There are four main parts to the AIX NetView/6000 console. The **menu** bar at the top is used to access AIX NetView/6000 tools and other applications. The top pictorial display is known as the **internet view** and shows all the networks and routers visible to AIX NetView/6000. The bottom pictorial, the **event card list** displays all the trap and event information logged by AIX NetView/6000. The event cards can also be displayed in a plain character format which is useful if the list is large. Lastly, the bottom of the display is an **information area** which is used to display messages during operation.

Double clicking on any of the objects in the *internet view* will display a corresponding **network view** and **segment view** containing the selected object. The window is shown in Figure 49 on page 99. The segment view is on the right containing all the IP addressable devices known to AIX NetView/6000 in that component of the network. Other AIX NetView/6000 operations are available from these interfaces by selecting the relevant network components.

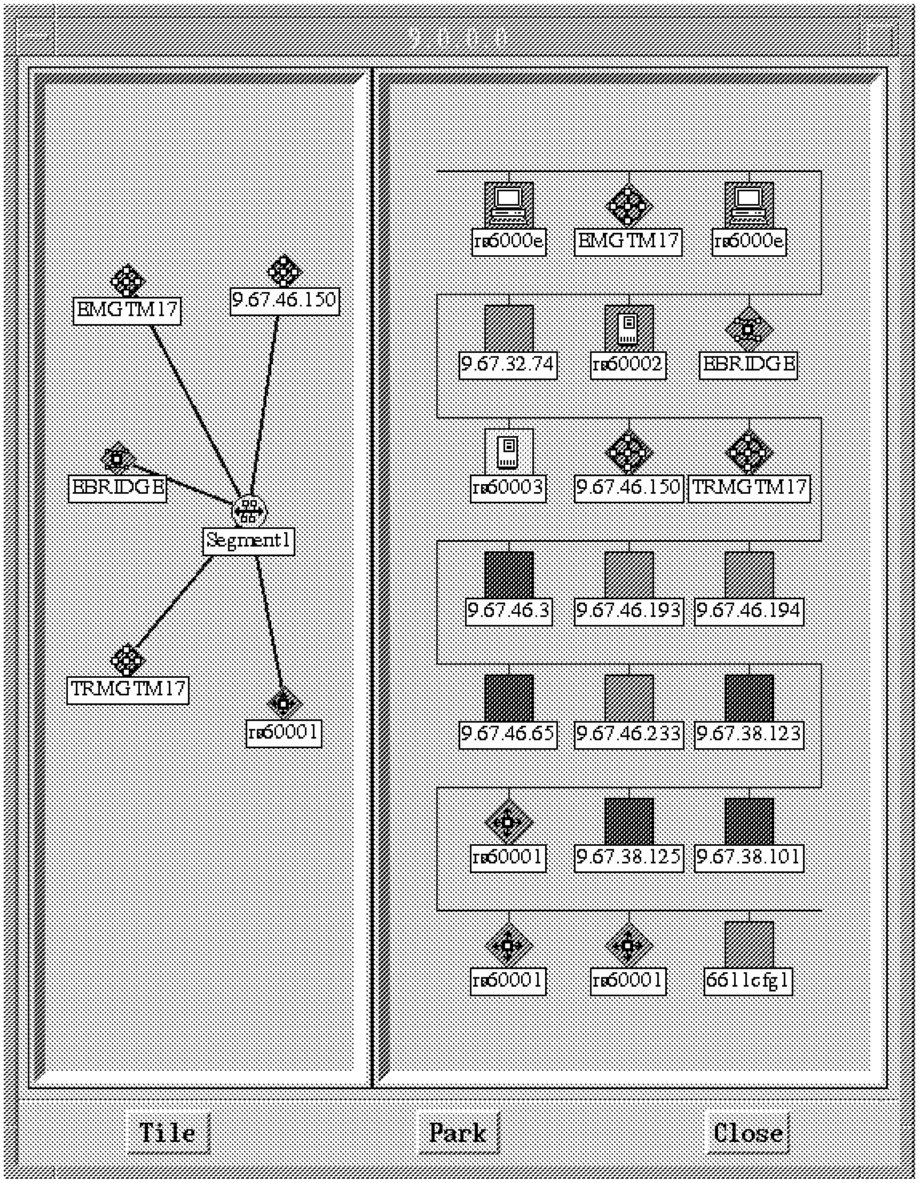


Figure 49. The AIX NetView/6000 Network and Segment Views

5.4 AIX NetView/6000 Information

AIX NetView/6000 has three sources of information:

- **AIX NetView/6000 Administration Reference**

  IBM Document Number SC31-6196

- **Overview and Examples of Using AIX NetView/6000**

  An ITSC Raleigh Redbook

  IBM Document Number GG24-3804

- The online **Help** and the AIX **InfoExplorer** product

Table 15 on page 100 shows the information source and the type of information provided.

Table 15 (Page 1 of 2). AIX NetView/6000 Information References

Information Source	**Type of Information Provided**
Administration Reference: product documentation available in printed form and through InfoExplorer*.	• Product overview: graphical user interface and operational behavior. • Initial installation and configuration information. • Managing SNA and TCP/IP networks. • Troubleshooting procedures for diagnosing problems. • AIX NetView/6000 reference pages.
Overview and Examples of Using AIX NetView/6000: documentation available in printed form.	• Overview of TCP/IP network management. • Overview of SNA network management. • AIX NetView/6000 positioning. • AIX NetView/6000 overview. • AIX NetView/6000 questions and answers. • AIX NetView/6000 installation comments. • Examples of using AIX NetView/6000 including example code and shell scripts.
Reference (man) pages: available in the Administration Reference (only in the printed form and InfoExplorer) and through the command line interface using the *man* command.	• AIX NetView/6000 commands. • AIX NetView/6000 daemons. • AIX NetView/6000 files. • AIX NetView/6000 xnm application.

Table 15 (Page 2 of 2). AIX NetView/6000 Information References

Information Source	Type of Information Provided
Online help: available by selecting *Help* from the menu bar.	• The **On Help** entry describes the options available from the Help pull-down menu. • **Task Help** alphabetically lists help entries for network management operations that you can select from the menu bar or context menus. Help entries are also provided for specific dialog boxes. • **Overview Help** alphabetically lists help entries that provide conceptual product information. • Access to the AIX NetView/6000 InfoExplorer database is available. • Access to the AIX Version 3.2 InfoExplorer database is available.

Part 2. 8250 Description, Installation, Configuration

Chapter 6. IBM 8250 Multiprotocol Intelligent Hub Overview

This chapter is an overview of the functions and facilities offered by the IBM 8250 Multiprotocol Intelligent Hub. It is intended to provide the reader with information about the following:

- Model description
- Advanced Backplane Architecture
- Fault tolerance
- Link redundancy
- Hot-pluggability
- Network management

Details about various 8250 media and management modules are given in the following chapters.

6.1 IBM 8250 Multiprotocol Intelligent Hub Description

The IBM 8250 Multiprotocol Intelligent Hub is a family of products designed to provide the platform to build local area networks meeting the requirements of customers 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).

The 8250 family consists of three models of rack mountable chassis, each offering an *Advanced Backplane Architecture*, which allows the concurrent operation of several LANs using various LAN protocols. A range of media and management modules are also provided to allow the design of networks addressing the individual needs of each organization.

8250 modules can be added, removed or reconfigured while the 8250 is in operation. This allows changes to the configuration of the network without affecting the operation of the other users on the network.

There are three different models of the IBM 8250 Multiprotocol Intelligent Hub.

6.1.1 IBM 8250 Model 017

This model has 17 slots for installing the various modules. It has been designed for rack mounting and comes with all the necessary hardware to install it in a rack. However, it can be installed anywhere within the building including on a table top, provided that the clearances necessary for proper operation and maintenance are provided.

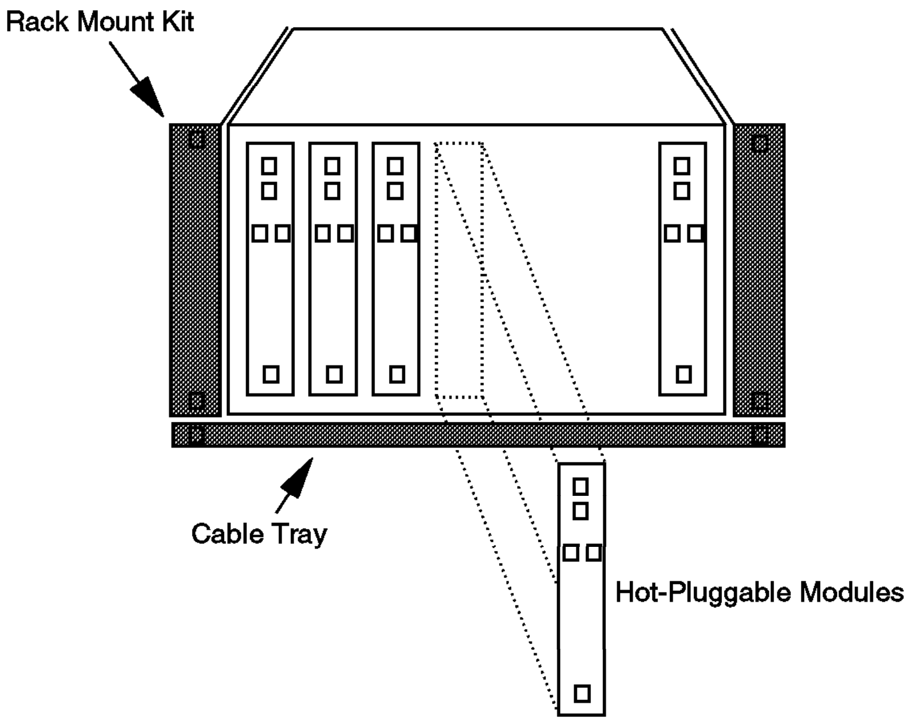


Figure 50. 8250 Model 017 Front Panel

Figure 50 depicts the front panel of an IBM 8250 Model 017. The slots are used to install the controller module(s), media modules and the management modules. Any slot on the 8250 can be used to install any module. Modules can be added, removed and reconfigured without powering down the 8250 or affecting the operation of the rest of the network. This means that new segments/networks/protocols can be added, or existing ones can be changed or removed without interrupting operation of the entire system.

Note that at least one slot is required for use by the controller module, leaving a maximum of 16 slots for the use by the media and management modules.

The 8250 Model 017 (P/N 43G3895) includes:

- One 17-slot hub chassis with built-in fan unit
- One power supply
- One fault-tolerant controller module
- One cable management tray
- One rack kit
- Attachment cables with adapters for XMM

A cable tray is provided with the IBM 8250 Model 17 so that cables attached to the modules can be run under the unit and out to the back where they will not be in the way. The tray also provides the required space between the bottom of the 8250 unit and the next device in the rack to ensure that there is adequate air flow to cool the unit.

If you choose not to install the cable tray, you must ensure that 1 3/4″ of space is open below the 8250 to ensure adequate airflow.

The rack mounting kit allows the IBM 8250 to be installed in a standard 19″ EIA rack.

The physical dimensions of the 8250 Model 017 are:

- 17.5″W x 18.3″D x 8.75″H

6.1.2 IBM 8250 Model 006

This model has 6 slots and is designed as a stand-alone unit to be located anywhere within the building. An optional rack mount kit is available for mounting the unit into a rack or onto a wall.

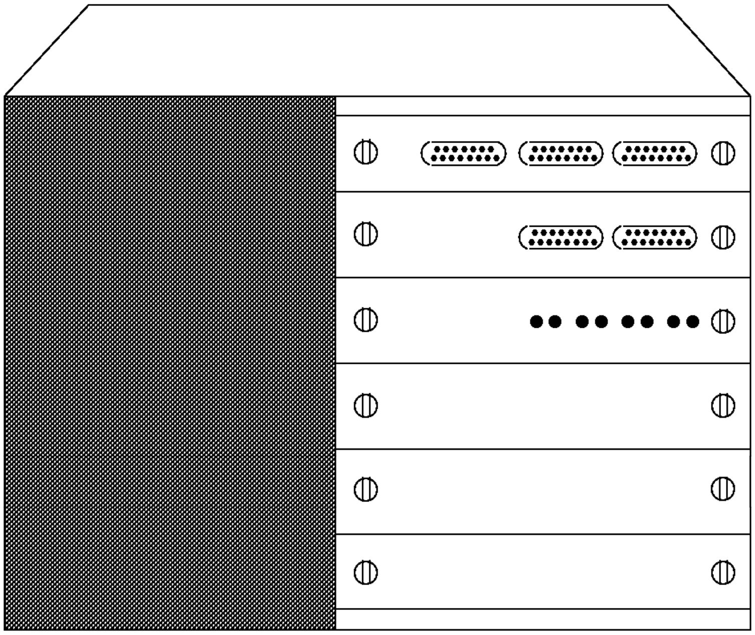


Figure 51. 8250 Model 006 Front Panel

Figure 51 depicts the front panel of an 8250 Model 006. The slots are used to install the controller module, media modules and the management modules. Any slot on the 8250 can be used to install any module. Modules can be added, removed and reconfigured without powering down the 8250 or affecting the rest of the network. This means that new segments/networks/protocols can be added, or existing ones can be changed or removed without interrupting the operation of the entire system.

Note that at least one slot is utilized by the controller module leaving a maximum of 5 slots to be used by the media and management modules.

The 8250 Model 006 Intelligent Hub (43G3892) includes:

- One 6-slot hub chassis

- One power supply
- One fault-tolerant controller module
- Attachment cables with adapters for XMM

A rack mounting kit is optional for the IBM 8250 Model 006 and has to be ordered separately if required (P/N 43G3798).

The physical dimensions of the 8250 Model 006 are:

- 16.7″W x 14.2″D x 6.9″H

Note that 8250 Model 006 has been withdrawn from the market and has been replaced by 8250 Model 6HC.

6.1.3 IBM 8250 Model 6HC

This model which supersedes the Model 006, has 6 slots and is designed as a stand-alone unit to be located anywhere within the building. An optional rack mount kit is available for mounting the unit into a rack or onto a wall. This model has a fault-tolerant controller module integrated into the chassis hence the name 6HC (Hidden Controller). This allows all 6 slots to be used for media and management module installation.

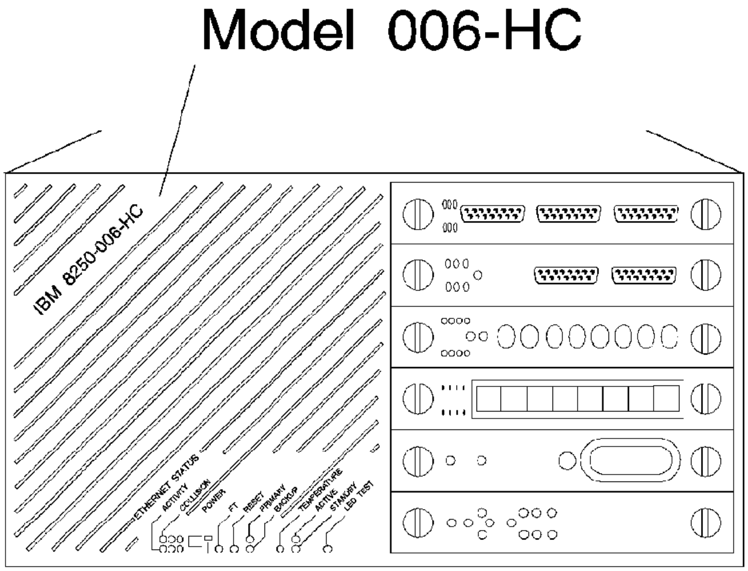


Figure 52. 8250 Model 6HC Front Panel

Figure 52 depicts the front panel of the IBM 8250 Model 6HC which has a number of media modules installed. The slots are used to install controller modules, media modules and the management modules. Any slot on the 8250 can be used to install any module. Modules can be added, removed and reconfigured without powering down the 8250 or affecting the operation of the rest of the network. This means that new segments/networks/protocols can be added, or existing ones can be changed or removed without interrupting the operation of the entire system.

The 8250 Model 6HC Intelligent Hub includes:

- One 6-slot hub chassis
- One power supply
- One integrated fault-tolerant controller module
- Attachment cables with adapters for XMM

A rack mounting kit is optional for the 8250 Model 6HC and has to be ordered separately if required (P/N 43G3798).

The physical dimensions of the 8250 Model 6HC are:

- 16.7″W x 14.2″D x 6.9″H

The 8250 Model 6HC has two buttons, and a number of LEDs on its front panel. For information about these buttons and LEDs, please refer to 6.6, “Model 6HC Controller Panel” on page 126.

6.2 Advanced Backplane Architecture

The IBM 8250 Multiprotocol Intelligent Hub uses an *Advanced Backplane Architecture* which provides the 8250 with the capability to run multiple networks using various protocols, concurrently. The maximum number of networks supported for each protocol are as follows:

- 3 Ethernet networks
- 7 token-ring networks
- 4 FDDI networks

Note that these numbers are the maximum number of networks which can exit on a single backplane when:

1. A management module is installed
2. A single type of protocol is used

More detailed information about the possible number of networks in a mixed protocol environment is provided below.

Modules can be assigned to a network using either the onboard dip switches (Ethernet modules only) or the network management module commands (all modules). Using dip switches requires the module to be removed from the 8250, while network assignment via a management module command can be done remotely and does not involve physical handling of the module.

Each module can also be set to *Isolated* mode. In this mode, the module is not connected to any network on the backplane, so the workstations connected to it can only communicate with each other. This can be used to create small isolated segments for security, testing or debugging purposes. Statistical information can not be collected from these *Isolated* segments. This is due to the fact that statistics gathering requires the attachment of a management module to the network, which is not possible in the case of an isolated module.

Some Ethernet modules provide *port switching* capability. This allows individual ports on a module to be assigned to different networks on the backplane. This feature provides a lot of flexibility when setting up, or changing the network topology.

The ability to take advantage of all the flexibility offered by the backplane architecture of the IBM 8250 Multiprotocol Intelligent Hub is limited if no management module is installed in the hub. The following limitations are applicable to an unmanaged IBM 8250 Multiprotocol Intelligent Hub:

- Only a single protocol (token-ring or Ethernet) is supported in an unmanaged 8250.
- The maximum number of available token-ring networks is 3 in 8250 Model 017 and 2 in 8250 Models 006 and 6HC.
- FDDI is not supported in an unmanaged 8250.

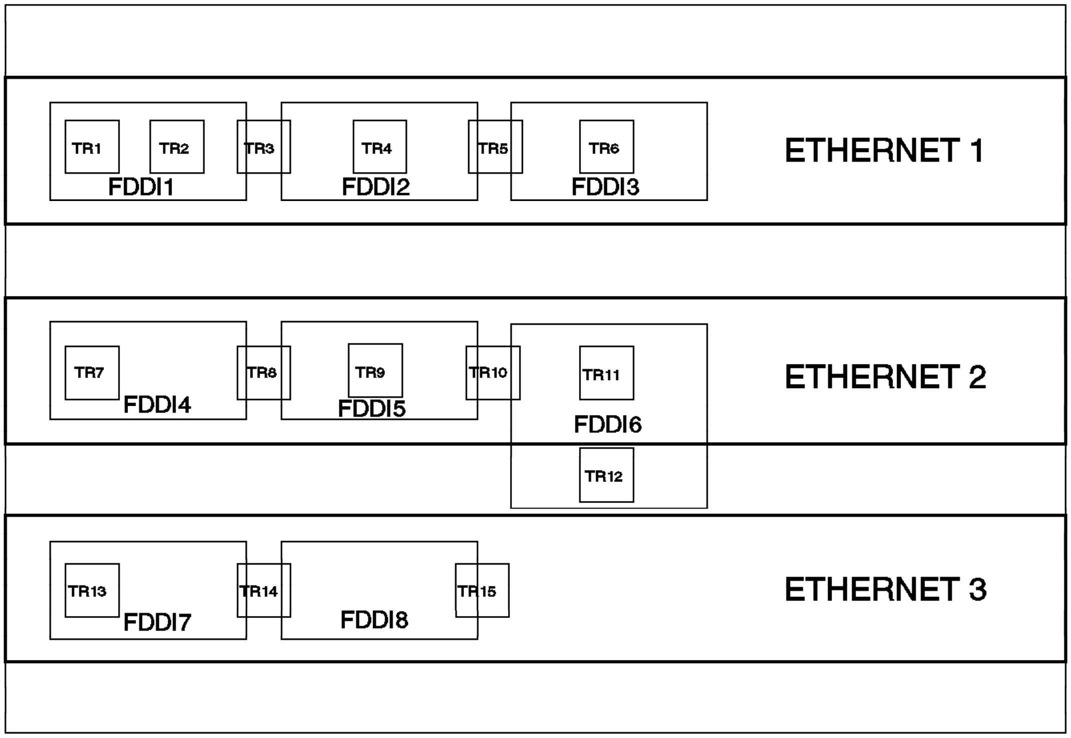


Figure 53. Advanced Backplane Architecture. How do token-ring, Ethernet and FDDI paths affect each other.

Figure 53 shows the the Advanced Backplane Architecture and how it can be used to accommodate multiple networks and protocols. The following is a description of the rules governing the use of the backplane:

1. There can be up to a maximum of three Ethernet networks supported on a single 8250. When three Ethernet networks (Ethernet_1 through Ethernet_3) are configured, you cannot have any other type of network (token-ring or FDDI) on that 8250.
2. There can be up to a maximum of 7 token-ring networks (token-ring_1 through token-ring_7) on a single 8250. When 7 token-ring networks are

configured, you can not have any other type of network (Ethernet or FDDI) on that 8250.

3. There can be up to a maximum of 4 FDDI networks (FDDI_1 through FDDI_4) on a single 8250. When 4 FDDI networks are configured, you can not have any other type of network (token-ring or Ethernet) on that 8250.

4. Each token-ring module which is assigned to one of the seven token-ring networks on the backplane, uses one of the resources called *token-ring path*. There are 15 token-ring paths on the backplane. They are referred to as *TR1* through *TR15* paths. The use of these paths affect the availability of Ethernet networks and FDDI path (FDDI path is explained below) as shown in the following table.

Table 16. Effects of Token-Ring Path Utilization on Ethernet and FDDI

Token-Ring Path	Takes Out
TR1	Ethernet_1, FDDI1
TR2	Ethernet_1, FDDI1
TR3	Ethernet_1, FDDI1, FDDI2
TR4	Ethernet_1, FDDI2
TR5	Ethernet_1, FDDI2, FDDI3
TR6	Ethernet_1, FDDI3
TR7	Ethernet_2, FDDI4
TR8	Ethernet_2, FDDI4, FDDI5
TR9	Ethernet_2, FDDI5
TR10	Ethernet_2, FDDI5, FDDI6
TR11	Ethernet_2, FDDI6
TR12	FDDI6
TR13	Ethernet_3, FDDI7
TR14	Ethernet_3, FDDI7, FDDI8
TR115	Ethernet_3, FDDI8

5. When you assign a token-ring module to one of the token-ring networks (token-ring_1 through token-ring_7), the 8250 will automatically allocate one of the available token-ring paths to this module. You can find out which token-ring paths on the backplane are used by using the management module SHOW NETWORK_PATHS command. However, you can neither choose the path used by the module, nor can you determine which path is used by a specific module.

6. The number of token-ring paths used by a single token-ring network depends on the number of token-ring modules on that network. Therefore, the minimum number of paths in a single token-ring network is 1 and the maximum is equal to the maximum number of token-ring modules that can be installed on the 8250.

Note

It is not common to have a token-ring network on the backplane that consists of a single module. Therefore, most 8250 publications refer to 2 paths as the minimum required to set up a token-ring network.

7. If one module is enough to set up the network that satisfies your requirement, it is advisable that you set the module to isolated mode, rather than assigning it to the backplane. This will save the use of backplane paths for use by other modules.

8. Each FDDI module which is assigned to one of the four FDDI networks on the backplane, uses one of the resources called *FDDI path*. There are 8 FDDI paths on the backplane. They are referred to as *FDDI1* through *FDDI8* paths. The use of these paths affect the availability of Ethernet networks and token-ring paths as shown in the following table.

Table 17. Effects of FDDI Paths Utilization on Ethernet and Token-Ring

FDDI Path	**Takes Out**
FDDI1	Ethernet_1, TR1, TR2, TR3
FDDI2	Ethernet_1, TR3, TR4, TR5
FDDI3	Ethernet_1, TR5, TR6
FDDI4	Ethernet_2, TR7, TR8
FDDI5	Ethernet_2, TR8, TR9, TR10
FDDI6	Ethernet_2, TR10, TR11, TR12
FDDI7	Ethernet_3, TR13, TR14
FDDI8	Ethernet_3, TR14, TR15

9. Similar to token-ring, assigning an FDDI module to one of the FDDI networks on the backplane will result in the 8250 allocating an FDDI path on the backplane to your module. You can find out which FDDI paths on the backplane are currently used by using the SHOW NETWORK_PATHS command. Note that early versions of TRMM (V.1.0 and V.1.1) do not display the FDDI paths. Like token-ring, you can not determine which paths is used by a specific module.

   The number of FDDI paths used by a single FDDI network depends on the number of FDDI modules on that network. Therefore, the minimum number of paths in a single FDDI network is 1 and the maximum is equal to the maximum number of FDDI modules that can be installed on the 8250.

10. Unlike token-ring and FDDI network, an Ethernet network consists of a single *path* regardless of the number of the modules which constitute that Ethernet network. Therefore, there are there Ethernet paths on the backplane and each one corresponds to an Ethernet network. The following table shows the effects of using Ethernet networks on the token-ring and FDDI paths.

Table 18. Effects of Ethernet Paths Utilization on FDDI and Token-Ring

Ethernet network	**Takes Out**
Ethernet_1	TR1, TR2, TR3, TR4, TR5, TR6, FDDI1, FDDI2, FDDI3
Ethernet_2	TR7, TR8, TR9, TR10, TR11, FDDI4, FDDI5, FDDI6
Ethernet_3	TR13, TR14, TR15, FDDI7, FDDI8

11. As can be seen from Figure 53 on page 110, the distribution of token-ring, FDDI and Ethernet paths over the backplane and the effects of their use on the other networks are uneven. For example, when you use Ethernet_1, you will lose the ability to utilize 6 token-ring paths (TR1 through TR6) and 3 FDDI paths (FDDI1 through FDDI3). On the other hand, the use of Ethernet_3 will

only take away three token-ring paths (TR13 through TR15) and 2 FDDI paths (FDDI7 and FDDI8). Therefore, when using multiple protocols on an 8250, it is best that you first assign the Ethernet modules to Ethernet_3 and then assign the modules for the other protocols.

12. When you set a module (token-ring, Ethernet or FDDI) to be isolated, that module is not connected to the backplane and does not take up any of the paths on the backplane.

13. Note that TR12 is a special case. It is not affected by the use of Ethernet_2, and its use does not affect Ethernet_2. However, using FDDI6 will render TR12 unavailable. Conversely, using TR12, will make FDDI6 unavailable.

Table 19 summarizes the maximum permitted combinations of different protocols in a single IBM 8250.

Ethernet	Token-Ring	FDDI
3	0	0
2	0	1
2	3	0
1	0	3
1	6	0
1	3	1
0	7	0
0	6	1
0	3	2
0	1	3
0	0	4

Table 19. Maximum Network Combinations in an IBM 8250

6.3 Fault Tolerance

The IBM 8250 Multiprotocol Intelligent Hub has a number of features to allow for the provision of highly available and fault-tolerant networks. These features are:

- Backup power supply
- Backup controller module
- Link redundancy
- Port switching
- Backup 8250
- Hot-pluggability

The following sections describe these features.

6.3.1 Backup Power Supply

All models of the IBM 8250 provide you with the ability to install an optional backup power supply. On the Model 017, the backup power unit (with its built-in fan unit) will be installed in place of the the second fan unit which is a standard feature of the 8250. This is shown in Figure 54.

On the Model 006 and 6HC, the backup power unit will be installed in the empty space available on the 8250. This requires you to remove a blank panel from the back to install the backup power unit. Note that the power unit between Model 017 and Model 006/6HC are not interchangeable.

Should the primary power supply fail, the backup power unit will automatically take over. The primary power unit can then be removed and replaced without affecting the operation of the network.

Note.

It will take 5 to 30 seconds (depending on the configuration of the 8250) to switch to the backup power supply. This may result in disrupting some of the existing sessions due to expiry of timers for those sessions.

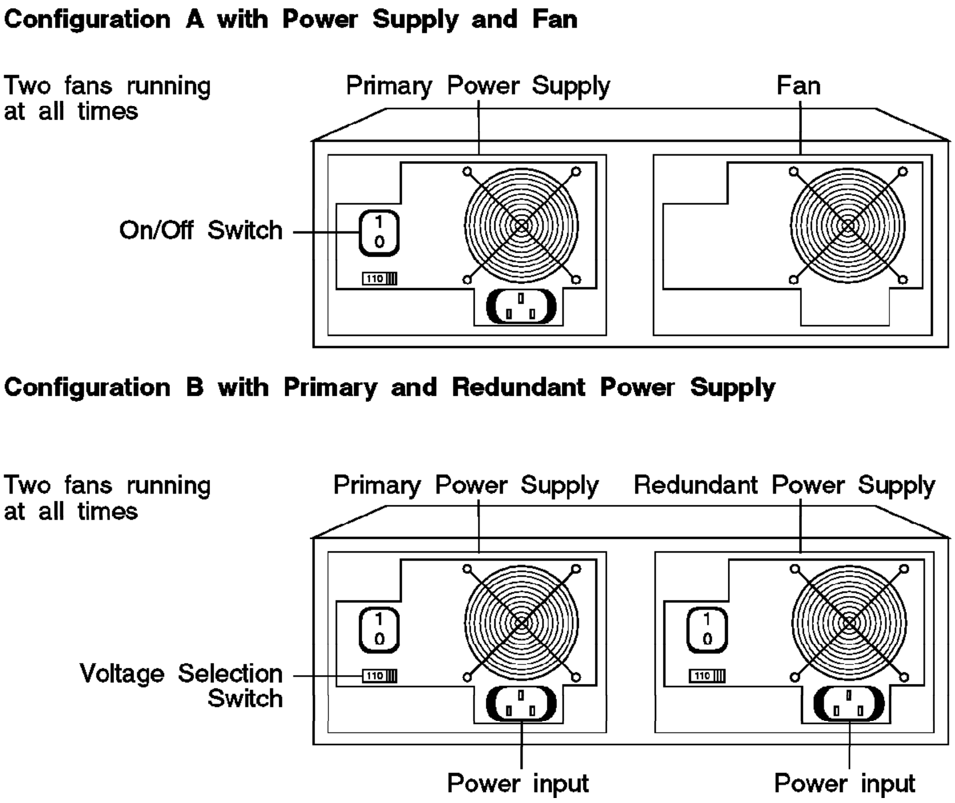

Configuration A with Power Supply and Fan
Two fans running at all times
Primary Power Supply
Fan
On/Off Switch
1
0
110
Configuration B with Primary and Redundant Power Supply
Two fans running at all times
Primary Power Supply
Redundant Power Supply
Voltage Selection Switch
1
0
110
1
0
110
Power input
Power input

Figure 54. Backup Power Supply

Should the backup power supply fail, the fault-tolerant controller module will attempt to switch back to the primary power supply. Therefore, once the primary power supply is replaced, you can leave the system running on the backup power supply until it is convenient to reset the 8250 to use the primary power supply.

Switching back to the primary power supply can be done by pressing the *power reset button* on the controller module or issuing the RESET POWER_SUPPLY command from the master management module.

LED displays on the active controller will provide the following information about the primary and backup power units:

- Whether or not the primary power unit is installed.
- Whether or not the backup power unit is installed.
- Whether the 8250 is currently working off the primary or the backup power unit.
- Whether the primary power unit has failed.
- Whether the backup power unit has failed.

Each power supply unit has two switches:

- Voltage Selection switch
- On/Off switch

> **Note**
>
> You should ensure that you set the voltage selection switch correctly during the installation of your 8250.

6.3.2 Backup Controller Module

By having a second controller module in the 8250, you can provide fault-tolerance in case of primary controller module failure. Like the backup power supply, switching to the backup controller module can take 5 to 30 seconds and may disrupt some of the existing sessions. For a full description of the controller module see 6.5, “Fault-Tolerant Controller Module” on page 123.

6.3.3 Link Redundancy

In order to provide an alternative connection between two 8250s which can be used in the event of a link failure, the Ethernet fiber modules implement a port redundancy feature. This requires you to provide for two physical links between the two 8250s. One of the links will be the *primary* link and the other will act as the *backup* link. This primary link will be active during the normal operation and will carry the traffic while the backup link will be idle. In the event of a problem with the primary link, an automatic switchover to the backup link will occur. This switchover will take less than 1/100 of a second allowing most operations to continue without any disruption. An example of a redundant cable configuration is shown in Figure 55 on page 116.

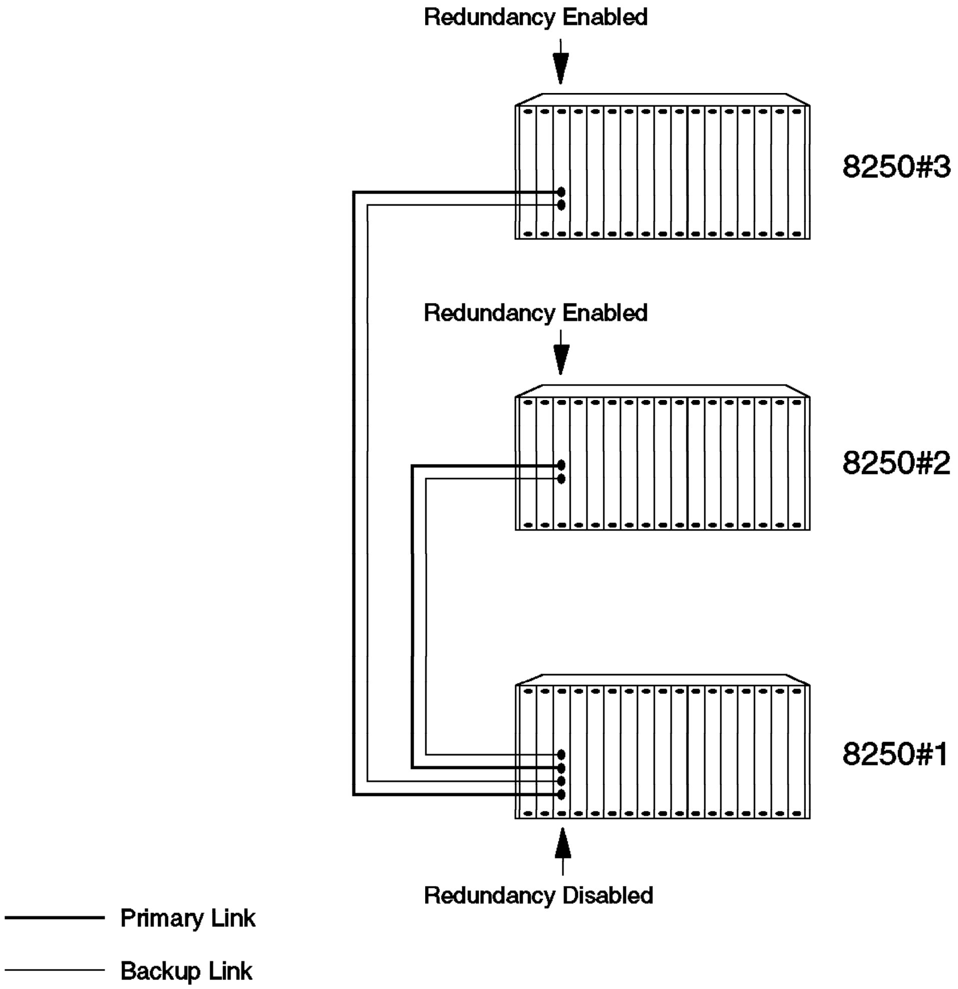


Figure 55. Star-Wired Fault Tolerant Network Configuration

The primary and backup port can be on the same module or on different modules in the same 8250.

Redundancy between the ports that are on the same module can be done using onboard dip switches or management module commands.

When using dip switches, port 2 can be designated as redundant port for port 1 and port 4 as redundant port for port 3. Using the management module allows any port to be designated as redundant to any other port on the same module.

To define cross-module redundancy within the same 8250 one of the following management modules are required to be installed on the 8250:

- Advanced Ethernet management module
- Advanced token-ring management module
- FDDI management module

The Ethernet fiber modules provide LED displays which show the operational status of each link and the status of redundancy settings for each port.

Note

The version of EMM advanced software that we used for our testing (V3.1) only allowed cross-module redundancy between ports of the same number. For example Slot 2, Port 2 could be redundant with Slot X, Port 2 but not Slot X, Port 3. This is not a restriction with later versions of the management module.

We did not have access to the Advanced token-ring management module at the time of writing the book.

Note that link redundancy should be enabled at one end of the link; otherwise, unpredictable results could happen.

6.3.4 Port Switching

Port switching allows individual ports on a module to be assigned to different networks on the backplane. This feature, which is available on certain Ethernet modules only, will provide you with the ability to design cost effective networks which will allow you to cater for configuration changes arising from the user relocations and component failures. Details about the modules which provide the port-switching feature can be found in Chapter 7, "8250 Ethernet Modules and Accessories" on page 129.

6.3.5 Backup 8250

By installing additional 8250s and taking advantage of port redundancy, you can ensure that the desired parts of your network will remain operational in case of the failure of an 8250.

For example, as explained in Chapter 9, "Ethernet Design Considerations" on page 205, we recommend that a network of multiple 8250s be connected in a star configuration. In this case, one 8250 will be acting as the concentration point for the whole network. Therefore, you are recommended to consider providing a backup 8250 for this central hub, so that the network will continue operating normally should this hub fail. Figure 56 on page 118 provides an an example of a backup 8250 in a star configuration.

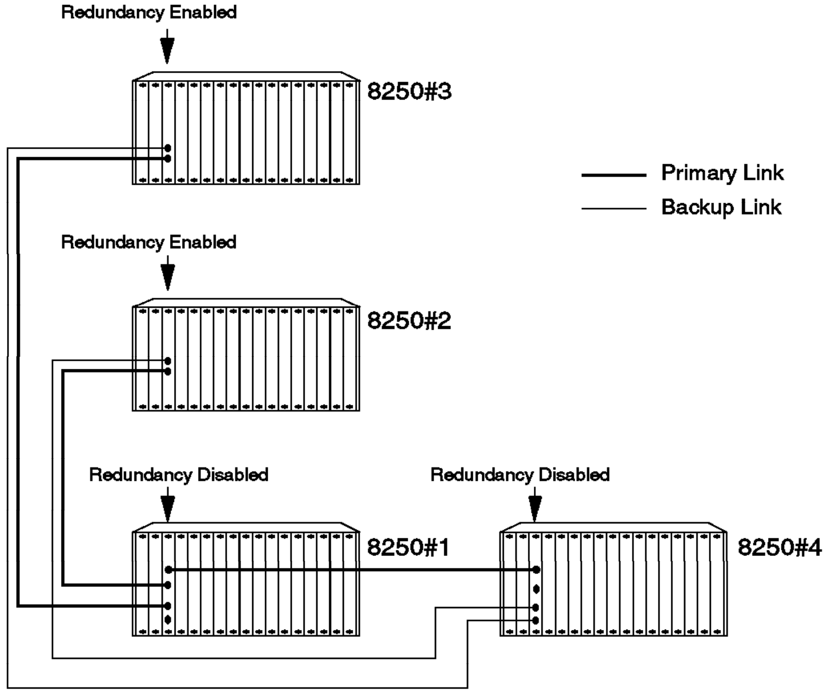


Figure 56. Backup 8250 in a Star Configuration

This example shows that by providing for an additional 8250 and using the link redundancy facility, the network can be configured so that in case of the failure of the primary 8250 (8250#1) the backup 8250 (8250#4) will take over automatically without disrupting the operation of the network.

Port redundancy should be enabled on 8250#2 and 8250#3 while it is disabled on the primary and backup concentrators. This will ensure that link switching will be performed by 8250#2 and 8250#3 when 8250#1 fails.

There should also be a link between the primary and backup 8250. This is required to ensure that the connectivity between the users on the network will be retained should the link between the primary and one of the other two 8250s (#2 or #3) fails.

For example, if the link between the primary (8250#1) and 8250#3 fails, the 8250#3 will switch the traffic to the backup link which is connected to 8250#4. In this case the traffic from users attached to 8250#3 will take the following route to reach the users attached to 8250#2:

```
        Backup Link                          Primary Link
8250#3 -------------->8250#4---------->8250#1------------->8250#2
```

6.3.6 Hot Pluggability

Any module in the 8250 can be removed or installed while the network is running without affecting the operation of the rest of the network. The only exception to this rule is the removal of the controller module if it is the only such module installed in the 8250.

A newly installed module will be configured according to its dip switch settings if there is no management module installed in the 8250. If a management module is present, for security reasons, a newly installed module will be set to isolated mode. This allows the network administrator to use the management module commands to set the attributes of the module and assign it to the desired network.

If a module of identical type is installed as a replacement for an existing module in an 8250 which has a management module, the new module will automatically be configured to be the same as the module that it replaces. This allows you to replace a failing module with an identical module and to restore the normal operation of your network within a very short space of time (time required to remove the faulty module and install the new module) without having to go through the process of discovering the configuration of the failed module and configuring the new module accordingly. This is made possible by the master management module, which has a copy of the configuration of every installed module in the 8250. The master management module will use this information to configure the new module if it is identical to the module which was previously installed in that slot.

Note

Our experience showed that with EMM 3.1, a replacement module is configured according to the last *saved* configuration, not the last *learned*.

When a management module is replaced on an 8250, the new management module will learn the configuration of the 8250 by *polling* each of the installed modules to learn their configuration.

Note that each management module has a set of device-dependent information which is not learned automatically and will need to be manually entered into a replacement management module via the ASCII terminal. More information about this is provided in 7.11, “Ethernet Management Module” on page 179.

Bridge and Ethernet Terminal Server modules have similar device-dependent information which need to be manually entered after the installation of these modules.

6.4 Network Management

The IBM 8250 provides a set of management modules which allow you to:

- Configure the media modules
- Collect fault information about the 8250 and its modules
- Collect statistics about the networks on the backplane

The following management modules are available:

- Ethernet management module
- Token-ring management module
- FDDI management module

A management module can be installed in any slot in the 8250 and like media modules can be assigned to an appropriate network on the 8250 backplane.

If more than one management module is installed in the 8250, one of them will become the *master* management module, while the others will become *slave* management modules.

The master and slave relationship is determined by the *mastership priority* which is assigned by the LAN administrator to each management module (via onboard dip switches on the management module or via the management module commands). The management module with the highest priority will become the master. If the master management module fails, the slave management module with the highest mastership priority will take over automatically.

If there is more than one management module with the same priority, one of them will become the master. Since in this case, it is not predictable which management module will become the master, you may have a situation where after a power-on, the management module which was the slave may become the master and since it may not have the latest configuration information about the 8250, your 8250 might be configured incorrectly. To avoid this situation, it is recommended that you should always ensure that different management modules within the same 8250 have different priorities and the one that you intend to be the master has the highest priority.

Also, when EMM is installed with other types of management modules (TRMM or FMM), you should ensure that a TRMM (or FMM) is the master. This is due to the fact that a TRMM (or FMM) acting as the master management module will always provide its slaves (TRMM, FMM and EMM) with the latest configuration information about the 8250, while the current version of EMM does not allow a master EMM to provide its slaves with configuration information. This configuration information is required by the slave TRMM modules to perform beacon recovery on the network that they are attached to.

A master management module can configure and detect faults on all the modules in the 8250. This includes modules attached to different networks, isolated modules and those running a different protocol than that of the management module. This enables you to use a single management module to configure and collect fault information about all the modules installed in the 8250 regardless of their type and protocol.

However, if you need to collect performance statistics about a network, a management module supporting that protocol type should be attached to that network. To collect a full range of statistics about networks which span several 8250s, one management module is required per 8250 per network.

6.4.1.1 Control Bus

As mentioned earlier, a single management module can manage all the media modules installed on an 8250. The communication between the management module and the media modules is via a dedicated *control bus*. As shown in Figure 57 each module has a connection to the control bus as well as to its designated network.

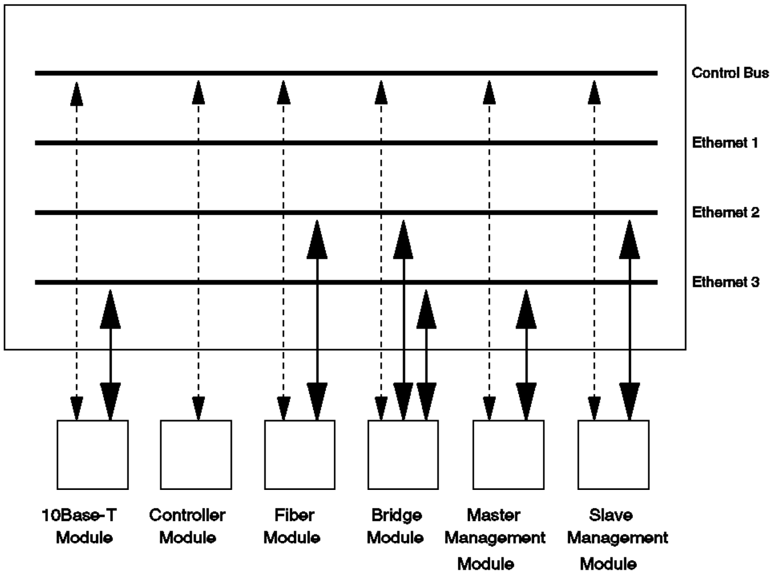


Figure 57. Control Bus

The master management module has control of the control bus and is the only one which can configure the media modules and detect faults. All the slave modules have access to the control bus for collecting performance statistics, but cannot configure the media modules or do fault detection.

6.4.1.2 Out-of-Band Management

Interface to the management modules can be provided via a local or remote ASCII terminal. The ASCII terminal connects to the management module via the RS-232 port provided on the module. Using the ASCII terminal, connected to the local management module, you can log in to the management module in a remote 8250 and provide configuration and fault detection as if you were locally attached to that 8250.

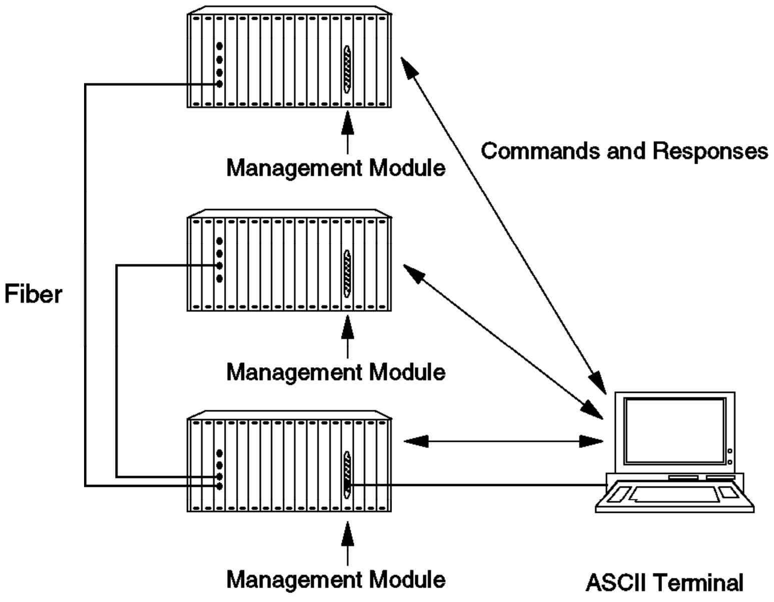


Figure 58. Out-of-Band Management

Figure 58 shows that by attaching an ASCII terminal to the RS-232 port on a management module, you can manage all the modules on that 8250 as well as the modules on the other 8250s connected to it.

To support this functionality, each 8250 will need to have a management module installed. The modules will also need to support the same virtual terminal protocol. This will be either *remote_login* (an 8250 proprietary protocol which should not to be confused with the remote_login protocol in UNIX environment) or *Telnet*.

Note

The current version of Ethernet management modules use a different virtual terminal protocol than token-ring and FDDI management modules. The Ethernet management modules use *remote_login* while the token-ring and FDDI management modules uses *Telnet*. Therefore, currently you can remotely log in to an Ethernet management module from another Ethernet management module only. Token-ring and FDDI management modules can be used to remotely log in to each other.

The remote_login protocol is not a routeable protocol; therefore, the two Ethernet management modules cannot communicate with each other via routers.

Remote_login is also implemented in the Ethernet bridge module.

6.4.1.3 In-Band Management

The management modules can also use SNMP over a TCP/IP network to communicate with an SNMP manager station such as AIX NetView Hub Management Program/6000. This allows you to integrate the management of the IBM 8250s with the management of other SNMP managed devices such as the IBM 6611 Network Processors.

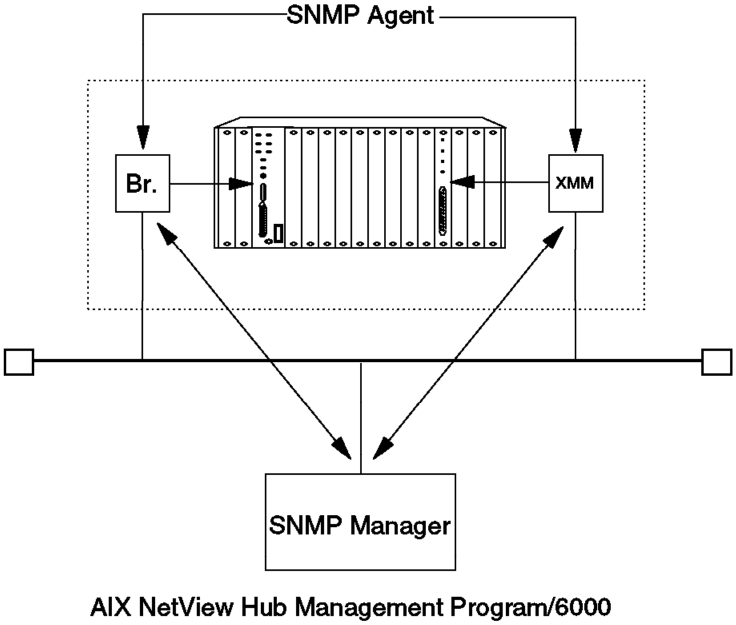


Figure 59. In-Band Management

Figure 59 is an overview of how the SNMP Manager in AIX NetView Hub Management Program/6000 communicates with the modules that contain SNMP agents.

For further details of this environment, refer to Chapter 13, “AIX NetView Hub Management Program/6000” on page 287.

6.5 Fault-Tolerant Controller Module

The fault-tolerant controller module provides synchronization and timing for all the modules in the 8250. It also monitors system activity and reports power supply failures and over-temperature conditions. An IBM 8250 will not operate without a controller module.

You can install an additional fault-tolerant controller module in the 8250 to provide backup for the primary controller module. The backup module will take over automatically (within 5 - 30 sec) in the event of the failure of the primary controller module.

Note

Model 6HC allows a fault-tolerant controller module to be installed as the backup for its integrated controller module. The interaction between the integrated controller module and the fault-tolerant controller module is exactly the same as the interaction between two fault-tolerant controller modules.

Figure 60 shows the front view of a fault-tolerant controller module.

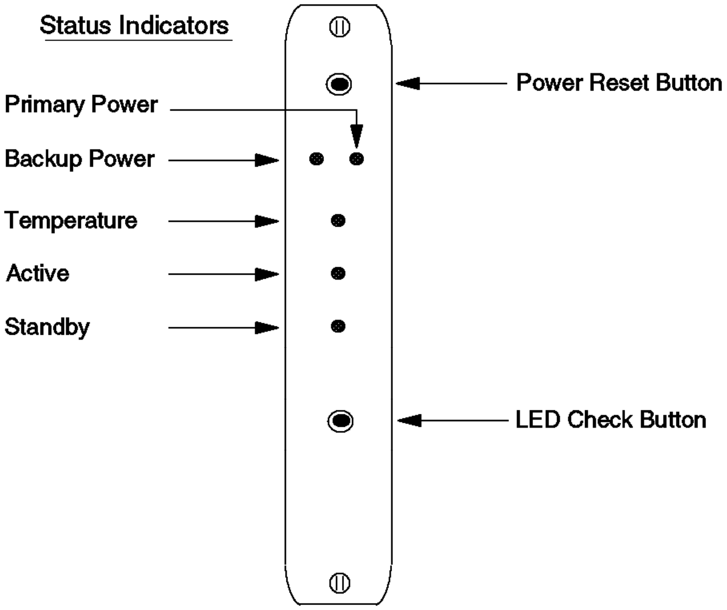


Figure 60. Front View of the Fault-Tolerant Controller Module

As can be seen, the controller module has two buttons and five LEDs on its front panel:

- **Power Reset button**

  Should the primary power supply fail, the 8250 will automatically switch to the backup power supply, if present. This allows you to remove and replace the primary power supply while the the network is operating. When the backup power supply is in use the **primary power LED** will blink indicating that the 8250 has switched to using the backup power supply. Once a new primary power supply has been installed, the *power reset button* can be pressed to restore the primary power supply as the working power.

  Note that using the XMM command RESET POWER_SUPPLY has the same effect as pressing the power reset button.

  If the 8250 is operating from the primary power supply, pressing this button will have no effect.

- **LED/Channel Check button**

  Pressing this button causes all the LEDs in all the modules in the 8250 to light up for approximately 5 seconds. Any LED that does not light up is defective.

After five seconds, the diagnostics continue with the network identification of all the modules. This causes each module's *port status LED* to blink a number of times indicating the network to which the port is assigned.

- 1 Blink - Port is configured for Network 1
- 2 Blinks - Port is configured for Network 2
- 3 Blinks - Port is configured for Network 3
- 4 Blinks - Port is configured for Network 4
- 5 Blinks - Port is configured for Network 5
- 6 Blinks - Port is configured for Network 6
- 7 Blinks - Port is configured for Network 7
- OFF - Port is isolated

This will be repeated five times. After the last sequence ends, the LEDs return to their normal state.

If you press this button while the diagnostics are in progress, the diagnostics will stop.

Note that the controller module LEDs stay *on* during the LED Channel/Check diagnostics since the controller module is connected to all the channels.

If you press this button twice more within one second of pressing it, you will force a backplane initialization. This procedure is used on an unmanaged 8250 (using token-ring) to ensure that a newly installed token-ring module is recognized by the existing token-ring modules.

A description of the controller module LEDs is given in the following table:

Table 20. Fault-Tolerant Controller LED Descriptions

LED name	Color	State	Description
Primary Power	Green	ON	Installed and OK.
		OFF	Not installed.
		Blinking	Has failed.
Backup Power	Green	ON	Installed and OK.
		OFF	Not installed.
		Blinking	Has failed.
Temperature	Green	OFF	Normal.
		ON	Temperature too high.
Active	Green	ON	This module is the active controller.
		OFF	This module is the standby controller.
Standby	Green	ON	This module is the active controller.
		OFF	This module is the standby controller.

6.5.1 Installing a Controller Module

The controller module does not require any configuration and the installation is, therefore, extremely simple.

1. Remove a blank panel on the concentrator to expose a slot.
2. Insert the module into the top and bottom board guides. Slide the module into the Concentrator.
3. Fasten the spring-loaded screws on the front of the module.

Controller module can be installed in any slot within the 8250.

6.6 Model 6HC Controller Panel

The 8250 Model 6HC has two buttons and a number of LEDs on its front panel:

- **Power Reset button**

  This button provides the same function as the similar button on the fault-tolerant controller module. Please refer to 6.5, "Fault-Tolerant Controller Module" on page 123 for more information about this button.

- **LED/Channel Check button**

  This button provides the same function as the similar button on the fault-tolerant controller module. Please refer to 6.5, "Fault-Tolerant Controller Module" on page 123 for more information about this button.

A description of the 8250 Model 6HC LEDs is given in the following table:

Table 21 (Page 1 of 2). LED Descriptions

LED name	Color	State	Description
FT	Green	OFF	The hub does not support backup power supply.
		ON	The hub supports backup power supply.
Primary Power	Green	ON	Installed and OK.
		OFF	Not installed.
		Blinking	Has failed.
Backup Power	Green	ON	Installed and OK.
		OFF	Not installed.
		Blinking	Has failed.
Temperature	Green	OFF	Normal.
		ON	Temperature too high.
Active	Green	ON	Integrated controller is active.
		OFF	Integrated controller is standby.
Standby	Green	ON	Integrated controller is standby.
		OFF	Integrated controller is active.

Table 21 (Page 2 of 2). LED Descriptions

LED name	Color	State	Description
Activity	Green	Blinking	Blinks briefly every time a packet is passed on the corresponding Ethernet Segment.
		ON	Constant activity on the corresponding Ethernet segment.
		OFF	No activity on the corresponding Ethernet segment.
Collision	Green	Blinking	Blinks briefly every time there is a collision on the corresponding Ethernet Segment.
		ON	Constant collision on the corresponding Ethernet segment.
		OFF	No collision on the corresponding Ethernet segment.

Note

There is one *collision* and one *activity* LED for each Ethernet segment. These LEDs do not apply to token-ring and FDDI segments.

Chapter 7. 8250 Ethernet Modules and Accessories

This chapter will describe the Ethernet modules for the IBM 8250 Multiprotocol Intelligent 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 8250 Ethernet modules are:

- Ethernet Fiber module
- Ethernet Fiber 2-port module with port-switching
- Ethernet Fiber 4-port module with port-switching
- Ethernet FOIRL Fiber module
- Ethernet 10BASE-T module
- Ethernet 12-port TELCO module
- Ethernet 24-port TELCO module
- Ethernet Transceiver module
- Ethernet Repeater module
- Ethernet BNC module
- Ethernet Bridge module
- Ethernet Management module

Ethernet transceivers which are available as accessories for the 8250, will also be described in this chapter. The current available transceivers are:

- 10BASE-T transceiver
- Fault-tolerant 10BASE-T transceiver
- Fiber Optic transceiver
- Fault-tolerant Fiber Optic transceiver
- FOIRL transceiver

7.1 Ethernet Modules Configuration Overview

To use the Ethernet modules installed in the IBM 8250, you must configure them to match your specific requirements. There are two ways of configuring these modules:

1. Setting dip switches on the module
2. Using management module commands

Using dip switches requires physical access to the module and can only be done after the module is removed from the concentrator (dip switches are not accessible when the module is mounted in the concentrator). The management module commands, on the other hand, allow you to configure the module without the need to handle the module physically. This provides you with the ability to configure the modules in an 8250 from a remote location.

When an IBM 8250 is powered on, it will be configured according to the last *saved* configuration information in the master management module. If there is no management module present, then each module will be configured according to its dip switch settings.

While the 8250 is in operation, new modules can be installed without affecting the operation of the existing users. Newly installed modules will be configured according to their dip switch settings if no management module is present. If a management module is already installed in the 8250, the newly installed module will be set to isolated mode allowing the administrators to use the management module commands to configure the module according to their requirements.

For Ethernet modules, with few exceptions, the same functions are offered by the dip switches and management module commands. However, this is not true of token-ring and FDDI modules. The functions offered by the dip switches are very limited in the case of token-ring and there are no dip switches available on the FDDI modules.

7.2 Ethernet Fiber Module

The Ethernet fiber module is a four-port module which provides fiber connectivity between the 8250s as well as fiber connectivity to-the-desk for the workstations in an Ethernet environment.

To provide fiber connectivity between two 8250s, the fiber module in one 8250 can be connected via a fiber cable to one of the following fiber modules in another 8250:

- Four-port fiber module
- Two-port fiber module with port-switching
- Four-port fiber module with port-switching

These modules use a synchronous signalling technique which is being adopted as the 10BASE-FB draft standard. This signalling technique is not compatible with the asynchronous signalling technique defined in the FOIRL standard. Therefore, the fiber module cannot be connected to IBM or third party concentrators using FOIRL compatible signalling.

The fiber module supports 50, 62.5, 85, and 100 micron fibers and comes with either ST, FC, or SMA-type connectors. You should use different part numbers and feature codes when ordering fiber modules with different connector types.

In general, on 62.5 micron cable, you can go up to 2000 meters point to point using the fiber modules. If you have poor quality cable, splices or many patch panels, you have to reduce this distance.

The four ports on the module can be configured to work either independently from each other or in *redundancy* mode.

If you configure redundancy by using dip switches, port 1 is paired with port 2 while port 3 is paired with port 4. In each pair, you set one of the links as the primary and the other as backup. During normal working condition, the primary link will carry the traffic, and the backup link will be idle. In case of a problem with the primary link, the switch-over to the backup link is automatic.

The setting of redundancy for ports 1 and 2 is independent from that of ports 3 and 4. For example, this will allow you to set port 2 as backup for port 1 while ports 3 and 4 can be set to operate in normal mode with no redundancy.

When you use the management module commands to set redundancy, there is no fixed pairing of the ports; therefore, any port on the fiber module can be set as the redundant port for any other port on the module. Also, if you use advanced management modules, you should be able to set port redundancy across different modules within the same 8250. For more information on port redundancy, please refer to 6.3.3, “Link Redundancy” on page 115.

This module can also be used to provide for fiber connectivity to the workstation. The workstation would need to connect via a fiber transceiver to the fiber link.

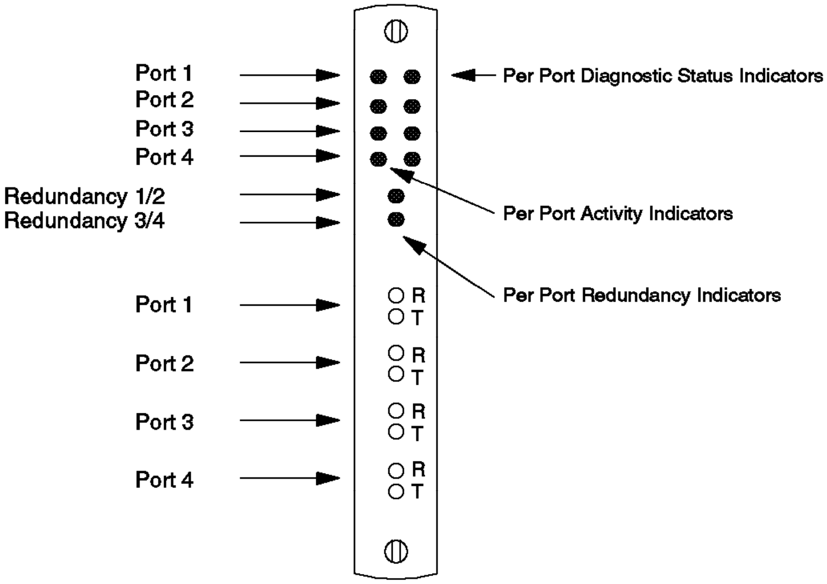

Port 1
Port 2
Port 3
Port 4
Redundancy 1/2
Redundancy 3/4
Port 1
Port 2
Port 3
Port 4
Per Port Diagnostic Status Indicators
Per Port Activity Indicators
Per Port Redundancy Indicators
R
T
R
T
R
T
R
T

Figure 61. Front View of the Four-Port Fiber Module

The fiber module has ten LEDs on the front panel that indicate the state of the module and its ports. The names and locations of these are shown in Figure 61. The following table describes what these indicators mean.

Table 22 (Page 1 of 2). Four-Port Fiber Module LED Descriptions

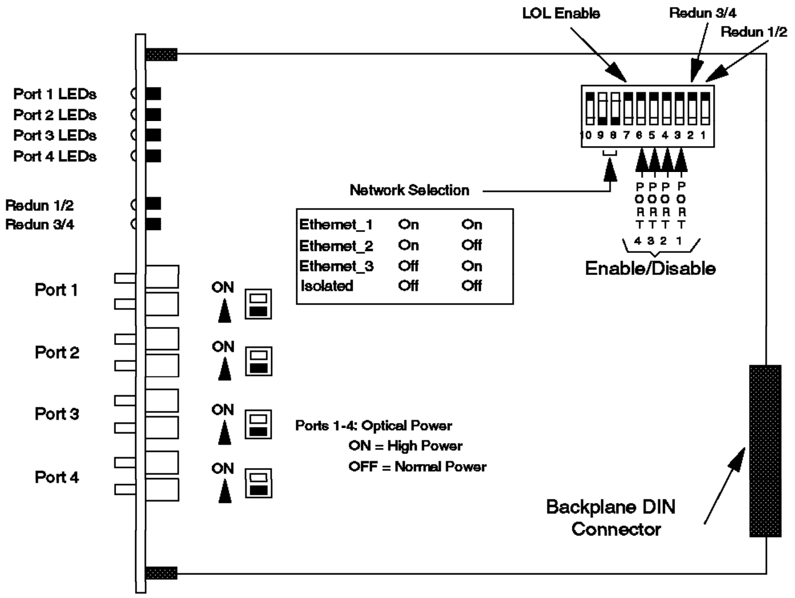
LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.

Table 22 (Page 2 of 2). Four-Port Fiber Module LED Descriptions

LED name	Color	State	Description
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		One blink	No light detected.
		Two blinks	Local jabber.
		Three blinks	Remote no light.
		Four blinks	Remote jabber.
		Five blinks	Invalid data received.
		Six blinks	Low light received.
Redundancy	Green	On	Enabled between ports 1/2, 3/4.
		Off	Disabled (ports are independent of each other).
		Blinking	Connection has been switched to backup link.

Further information about the meaning of LEDs is provided in the installation material shipped with the module.

Figure 62 shows the side view of the fiber module including its dip switches, their meanings and the factory settings.



Ethernet_1	On	On
Ethernet_2	On	Off
Ethernet_3	Off	On
Isolated	Off	Off

Ports 1-4: Optical Power
ON = High Power
OFF = Normal Power

Figure 62. Side View of the Four-Port Fiber Module

7.2.1 Configuring Fiber Module

To configure the fiber module, you must do the following:

- Set optical power to *High* or *Normal*

  The high power setting allows you to have longer distances of fiber cable. It is recommended that you should normally use the *normal* setting (factory default) for the optical power.

  The optical power for this module can only be set via dip switches and can not be overridden by management module commands.

- Assign the module to a network

  All the ports on this module must be assigned to the same network (as opposed to the port-switching fiber modules which allow each port to be assigned to any network independently from the assignment of the other ports on the module). The network assignment allows you to attach all the ports on this module to Ethernet_1, Ethernet_2, Ethernet_3 or isolated. When isolated, the ports on this module can only communicate with each other. Network assignment can be done using dip switches or the following management module command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

- Enable/disable ports

  Each port can be enabled/disabled independently from the other ports. This can be done using dip switches or the following management module command:

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

- Enable/disable port redundancy

  You can enable/disable link redundancy between ports on the fiber module to provide backup in case of link/port failure. Note that when you enable port redundancy, the setting of port enable/disable switches for these ports is ignored. You must also ensure that port redundancy is set at one end of the link only, to prevent unpredictable results. Port redundancy can be set via dip switches or the following management module command:

  ```
  SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}
  ```

- Enable/disable low light detection

  This allows you to enable/disable low light detection on all the ports. Low light is defined as power received between -26.0 dBm and -30.0 dBm peak power and can be used to enable the fiber module to indicate the *low light* conditions via the status LEDs on the front panel. Low light warning can be set via dip switches or the following management module command:

  ```
  SET MODULE {slot} LOW_LIGHT_WARNING {enable/disable}
  ```

7.2.2 Configuration Example

Figure 63 on page 134 is an example of using fiber modules to set up a star topology of 8250s to connect two buildings together. Note that there are two fiber modules in the primary concentrator (hub of the star), and by connecting those two modules to the same Ethernet network, we can set up the entire network as one LAN and ensure that all the workstations can communicate with each other.

In this configuration, you could also have taken advantage of port redundancy offered by the fiber modules by setting up additional links between the 8250s. This would have allowed you to ensure continuation of service in case of link or port failures on the fiber modules.

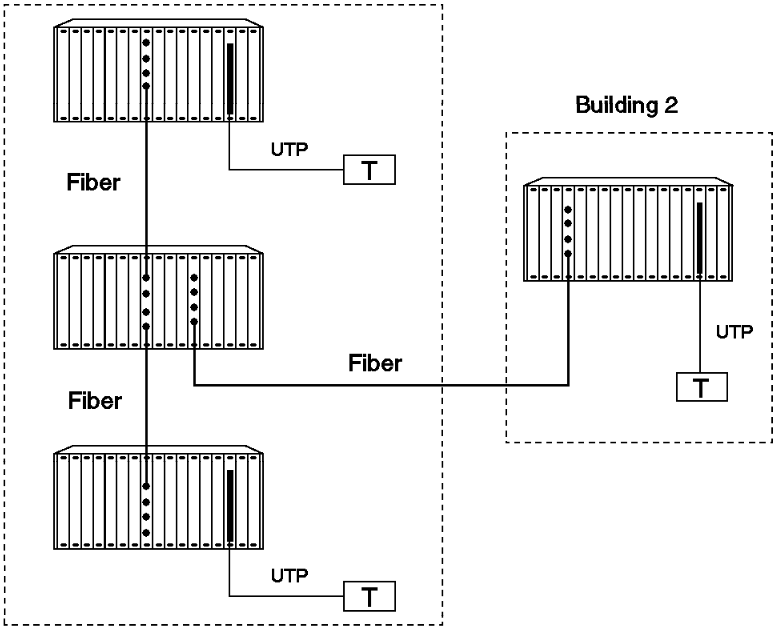
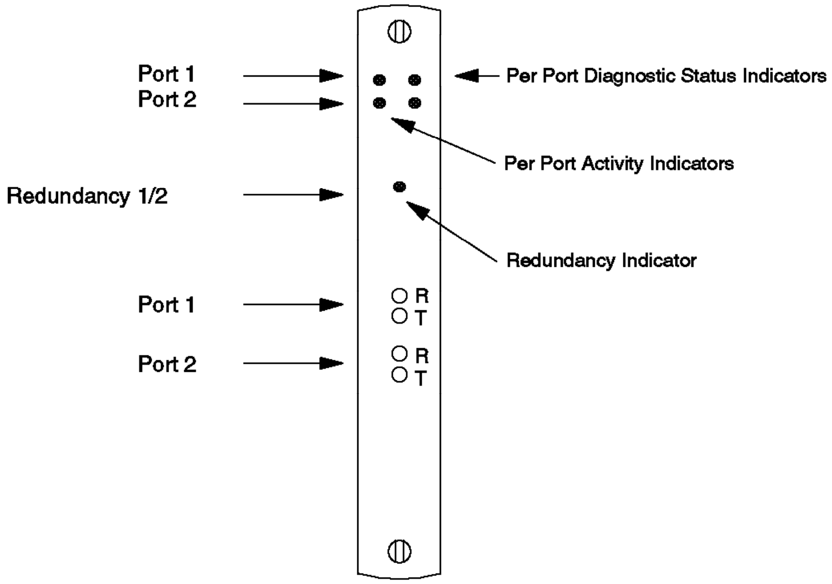


Figure 63. Configuration Example for Fiber Module

7.3 Two-Port Fiber Module with Port Switching

This is a a two-port module which provides fiber connectivity between the 8250s as well as fiber connectivity for the workstations in an Ethernet environment.

In terms of functionality, the port switching fiber module is identical to the fiber module with the exception that each port can independently be attached to any Ethernet network on the backplane or can be isolated. Port switching can be done via onboard dip switches or by issuing commands to a management module. Using the management module allows you to switch the users from one network to the another without having to visit the wiring closet or touch the patch panel.


Port 1
Port 2
Per Port Diagnostic Status Indicators
Per Port Activity Indicators
Redundancy 1/2
Redundancy Indicator
Port 1
R
T
Port 2
R
T

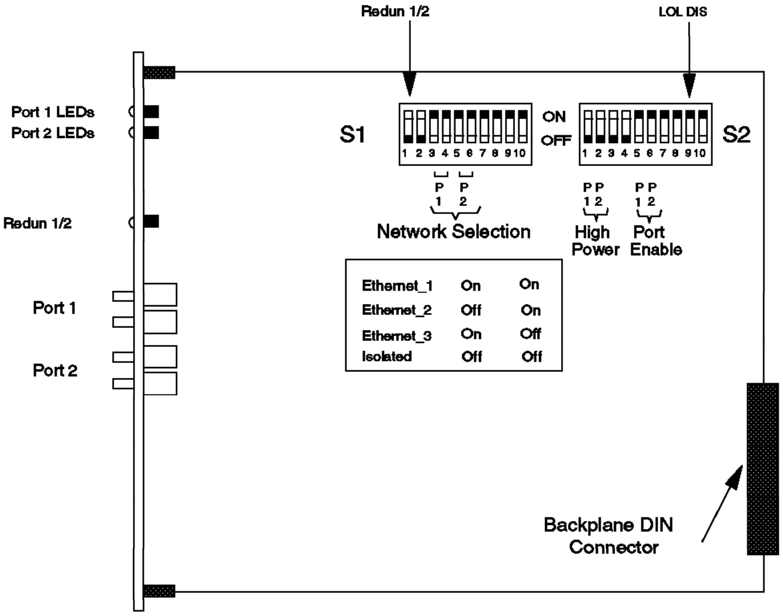
with Port Switching

Figure 64. Front View of the Two-Port Fiber Module

The two-port fiber module with port switching has five LEDs on the front panel that indicate the state of the module and its ports. The names and locations of these are shown in Figure 64. The following table describes what these indicators mean.

Table 23. Two-Port Fiber Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		One blink	No light detected.
		Two blinks	Local jabber.
		Three blinks	Remote no light.
		Four blinks	Remote jabber.
		Five blinks	Invalid data received.
		Six blinks	Low light received.
Redundancy	Green	On	Enabled between ports 1/2.
		Off	Disabled (ports are independent of each other).
		Blinking	Connection has been switched to backup link.



Ethernet_1	On	On
Ethernet_2	Off	On
Ethernet_3	On	Off
Isolated	Off	Off

with Port Switching

Figure 65. Side View of the Two-Port Fiber Module

Figure 65 shows a side view of the two-port fiber module with its dip switches, their meanings and the factory settings. Notice that there is one set of channel select dip switches per port.

7.3.1 Configuring Two-Port Fiber Module with Port Switching

To configure this module you must do the following:

- Assign the ports to a network

  The ports on the port-switching fiber module can be assigned to any Ethernet network independently from the assignment of the other ports on the module. The ports can be assigned to Ethernet_1, Ethernet_2, Ethernet_3 or isolated. The network assignment can be done via dip switches or the following management module command:

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

- Enable/disable ports

  Each port can be enabled/disabled independently from the other port. This can be done via dip switches or the following management command:

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

- Enable/disable link redundancy

  You can enable/disable link redundancy between ports on the module to provide backup in case of link/port failure. When you enable redundancy, the setting of enable/disable switches for these ports is ignored. You must also ensure that port redundancy is set at one end of the link only, to avoid unpredictable results. Port redundancy can be set via dip switches or the following management module command:

  ```
  SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}
  ```

- Enable/disable low light detection

This allows you to enable/disable low light detection on both ports. Low light is defined as power received between -26.0 dBm and -30.0 dBm peak power. Low light warning can be set via dip switch or the following management module command:

```
SET PORT {slot.port} Low_Light_Warning (enable/disable)
```

- Set optical Power to *High* or *Normal*

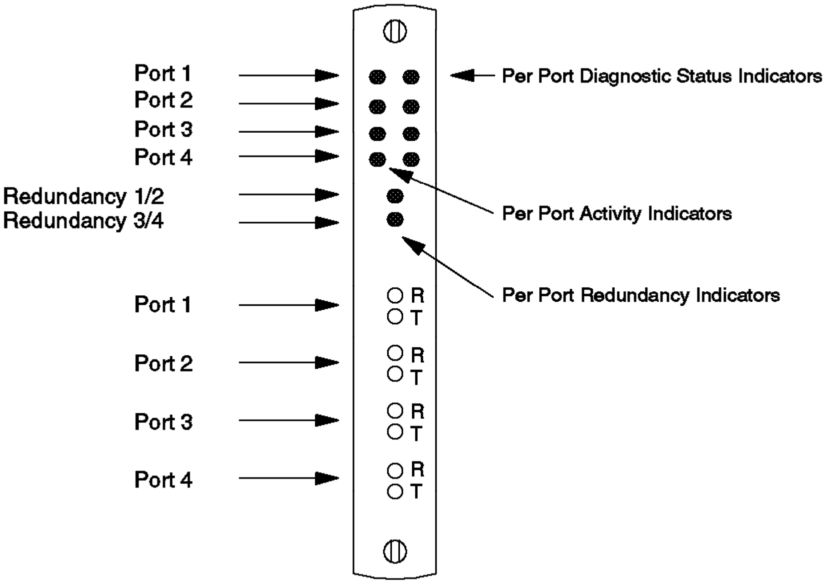
  The high power setting allows you to have longer distances of fiber cable. It is recommended that you should normally use the *normal* setting (factory default) for the optical power. This can be set via dip switches or the following management module command:

  ```
  SET PORT {slot.port} High_Power {enable/disable}
  ```

7.4 Four-Port Fiber Module with Port Switching

This is a four-port module which provides fiber connectivity between the 8250s as well as fiber connectivity for the workstations in an Ethernet environment.

Apart from the fact that it provides four ports rather than two it is identical to the two-port fiber module with port switching.


Port 1
Port 2
Port 3
Port 4
Redundancy 1/2
Redundancy 3/4
Per Port Diagnostic Status Indicators
Per Port Activity Indicators
Per Port Redundancy Indicators
Port 1
Port 2
Port 3
Port 4
R
T
R
T
R
T
R
T

with Port Switching

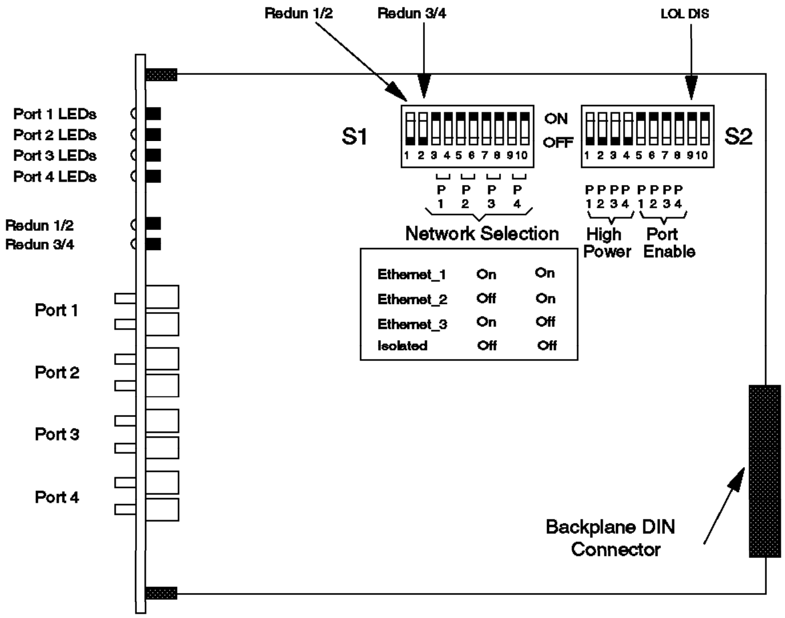
Figure 66. Front View of the Four-Port Fiber Module

This module has 10 LEDs on the front panel that indicate the state of the module and its ports. The names and locations of these are shown in Figure 66. The following table describes what these indicators mean.

Table 24. Four-Port Fiber Module (with Port Switching) LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		One blink	No light detected.
		Two blinks	Local jabber.
		Three blinks	Remote no light.
		Four blinks	Remote jabber.
		Five blinks	Invalid data received.
		Six blinks	Low light received.
Redundancy	Green	On	Enabled between ports 1/2, 3/4
		Off	Disabled (ports are independent of each other)
		Blinking	Connection has been switched to backup link.

Figure 67 shows the Module's dip switches, their meanings and the factory settings.



Ethernet_1	On	On
Ethernet_2	Off	On
Ethernet_3	On	Off
Isolated	Off	Off

with Port Switching

Figure 67. Side View of the Four-Port Module

7.4.1 Configuring Four-Port Fiber Module with Port Switching

The configuration steps are the same as for the two-port fiber module with port switching. Please see 7.3.1, “Configuring Two-Port Fiber Module with Port Switching” on page 136 for details.

7.5 Ethernet FOIRL Fiber Module

The Ethernet FOIRL fiber module is a four-port, fiber repeater module which provides fiber connectivity between the 8250s as well as between the 8250 and third party products implementing the FOIRL (Fiber Optic Inter Repeater Link) standard. This module can also provide direct FOIRL connectivity for the workstations.

To provide fiber connectivity between two 8250s, the FOIRL fiber module in one 8250 should be connected via fiber cable to the FOIRL fiber module in the other 8250.

Note: The FOIRL module uses an *asynchronous* signalling which is not compatible with the *synchronous* signalling used by the following 8250 fiber modules:

- Four-port fiber module
- Two-port fiber module with port-switching
- Four-port fiber module with port-switching

The FOIRL module is recommended to be used primarily to connect 8250s to other manufacturer′s concentrators which are FOIRL compatible. For connecting 8250s together, it is recommended that you use 8250 fiber modules which use the synchronous signalling and offer superior functionality when compared to FOIRL modules. For example, an FOIRL module will act as a 1/2 repeater when connecting two 8250s together, while the fiber modules have no repeater presence.

To provide fiber connectivity for the workstations, this module can be connected to FOIRL transceivers which are in turn connected to the workstation.

In general, on 62.5 micron cable, you can go up to 2000 meters point to point using the FOIRL modules. If you have poor quality cable, splices or many patch panels, you have to reduce this distance.

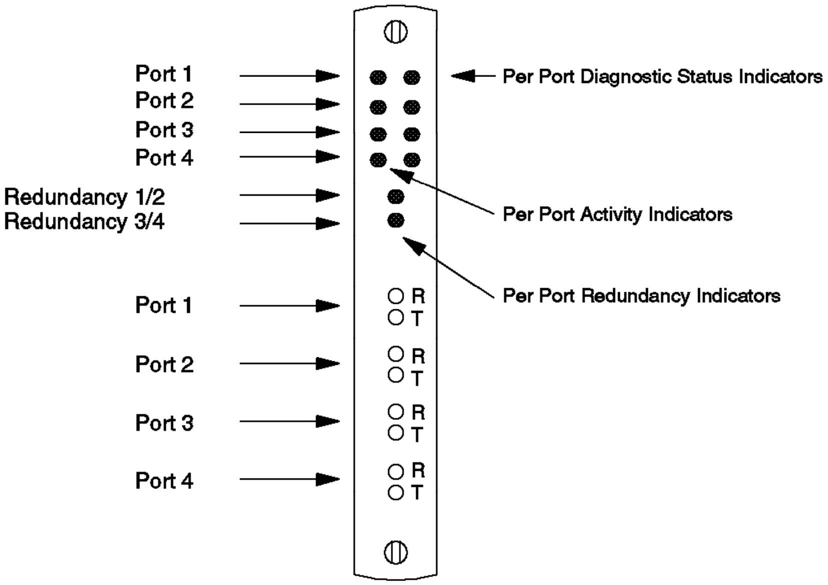

Port 1
Port 2
Port 3
Port 4
Redundancy 1/2
Redundancy 3/4
Port 1
Port 2
Port 3
Port 4
Per Port Diagnostic Status Indicators
Per Port Activity Indicators
Per Port Redundancy Indicators
R
T
R
T
R
T
R
T

Figure 68. Front View of the FOIRL Fiber Module

This module has ten LEDs on the front panel that indicate the state of the module and its ports. The names and locations of these are shown in Figure 68. The following table describes what these indicators mean.

Table 25. FOIRL Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		One blink	No light detected.
		Two blinks	Local jabber.
		Three blinks	Remote no light.
		Four blinks	Remote jabber.
		Five blinks	Invalid data received.
		Six blinks	Low light received.
Redundancy	Green	On	Enabled between ports 1/2, 3/4.
		Off	Disabled (ports are independent of each other).
		Blinking	Connection has been switched to backup link.

Figure 69 on page 141 shows the FOIRL module dip switches, their meanings and the factory settings. Note that the setting of all the switches can be overridden, remotely, via a management module.

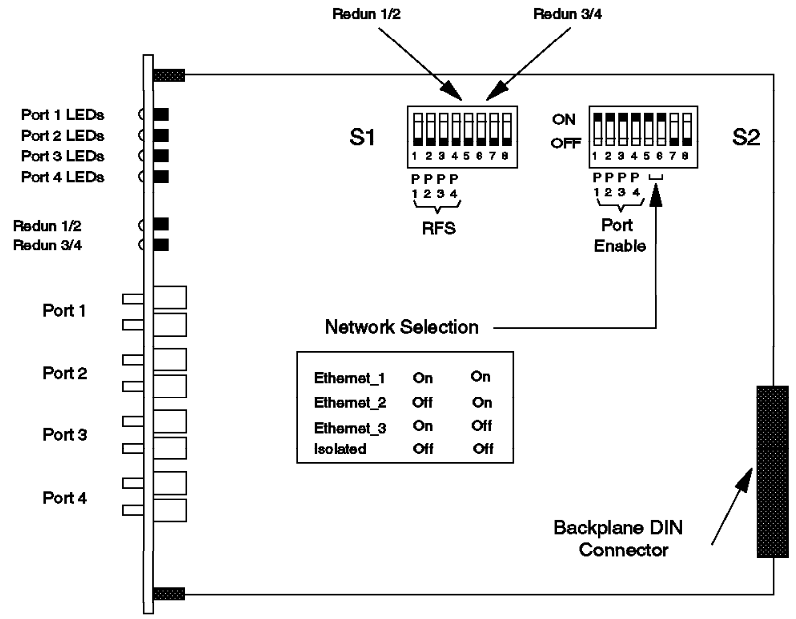


Figure 69. Side View of the FOIRL Module

7.5.1 Configuring the FOIRL Module

To configure the FOIRL module, you must do the following:

- Assign the module to a network

  The module should be assigned to a network or set in isolated mode. As this module does not provides per port switching, all the ports on the module will be assigned to the same network. This can be done via dip switches or the following management module command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

- Enable/disable ports

  Each port can be enabled/disabled independently from the other ports. This can be done via dip switches or the following management module command:

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

- Enable/disable redundancy

  If you have a management module installed, you can enable or disable port redundancy between any two ports on the module. If you do not have a management module, you can use the dip switches on the module to configure port redundancy between ports 1 and 2 and/or ports 3 and 4. The format of the management module command is as follows:

  ```
  SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}
  ```

  In port redundancy, you set one of the links as the primary and the other as backup. during normal working condition, the primary link will carry the traffic, and the backup link will be idle. In case of a problem with the primary link, the switch-over to the backup link is automatic.

Note that enabling port redundancy for two ports automatically enables the ports themselves, even if the ports were previously disabled.

You must ensure that you enable port redundancy on only one end of the link. The other end of the redundant link must have *Remote Failure Signalling* (RFS) enabled.

- Enable Remote Failure Signalling for port redundancy

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

  When you connect two FOIRL modules and enable port redundancy between two ports on one of the modules at the end of the links, you must enable Remote Failure Signalling for the ports on the module at the other end of the links. This is required because when using FOIRL, *no light* and *partition* errors can be detected on the receive path of a redundant port, but can not be detected on the transmit path (due to the asynchronous signalling technique used in the FOIRL standard). RFS provides a way for transmit failures to be detected so that a switch-over from a primary to a backup port can occur.

  As can be noticed, the fiber modules (due to use of synchronous signalling technique) do not require a functions similar to the RFS function. This is because, in 10BASE-FB, a 2.5 MHz active idle signalling technique is used to indicate that the transmit path is idle. In addition, the transmit data signal is synchronized to this idle signal, enabling the receiving MAU to remain locked to the active idle/packet data transitions. In this way, a module at one end of the link would be able to detect *no light* and *partition* for both the transmit and receive paths.

7.5.2 10BASE-T Module

The 10BASE-T module is an eight-port IEEE 802.3 repeater module that complies with the 10BASE-T standard and supports backbone and to-the-desk connectivity over both UTP and STP. A single module can support any mix of UTP and STP connections.

Note that STP support provided by the 8250 on the 10BASE-T modules is not part of the 10BASE-T standard.

Maximum distances support by each port are:

- 150 m on 22 gauge UTP cable
- 125 m on 24 gauge UTP cable
- 100 m on 26 gauge UTP cable
- 200 m on IBM Type 1 cable

In addition to complying with the 10BASE-T standard, each port supports a number of non-10BASE-T features to support the connection of equipment that does not fully conform to the 10BASE-T standard. These features are:

1. Normal/low squelch mode

   Allows you to set low *squelch* level which enables you to increase achievable distances by 25% to 50%.

2. Link integrity

   Allows *link integrity* to be disabled for communication with older equipment which does not support link integrity.

3. STP support

   Provides support for shielded twisted pair (STP) connection on any port for both backbone and to-the-desk connectivity.

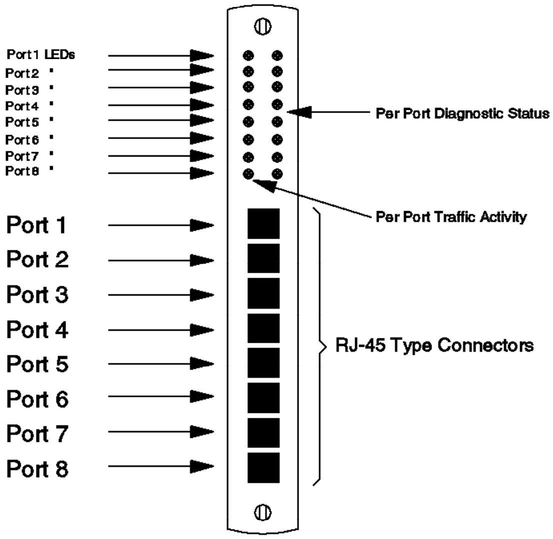


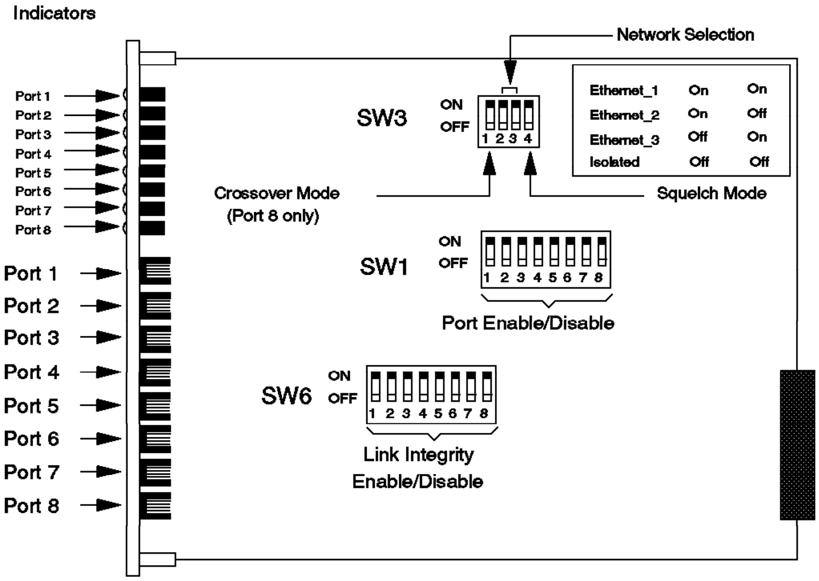
Figure 70. Front View of the 10BASE-T Module

This module has 16 LEDs on the front panel that indicate the state of the module and its ports. The names and locations of these are shown in Figure 70. The following table describes what these indicators mean.

Table 26. 10BASE-T 8-Port Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		One blink	Link integrity error.
		Two blinks	Jabber error or port partitioning.
		Timed blinks	Link integrity disabled.

Figure 71 on page 144 shows the side view of a 10BASE-T module including its dip switches, their meanings and the factory settings.



Ethernet_1	On	On
Ethernet_2	On	Off
Ethernet_3	Off	On
Isolated	Off	Off

Figure 71. Side View of the 10BASE-T Module

7.5.3 Configuring 10BASE-T Module

To configure the 10BASE-T module, you must do the following:

- Assign the module to a network

  All the ports on this module must be assigned to the same network. The network assignment allows you to attach all the ports on this module to Ethernet_1, Ethernet_2, Ethernet_3 or isolated. When isolated, the ports on this module can only communicate with each other. To assign the module to a network, you can use dip switches or the following network management command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

- Enable/disable any of the 8 ports

  Each port can be enabled/disabled independently from the other ports. This can be done via dip switches or the following management module commands:

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

- Enable/disable link integrity

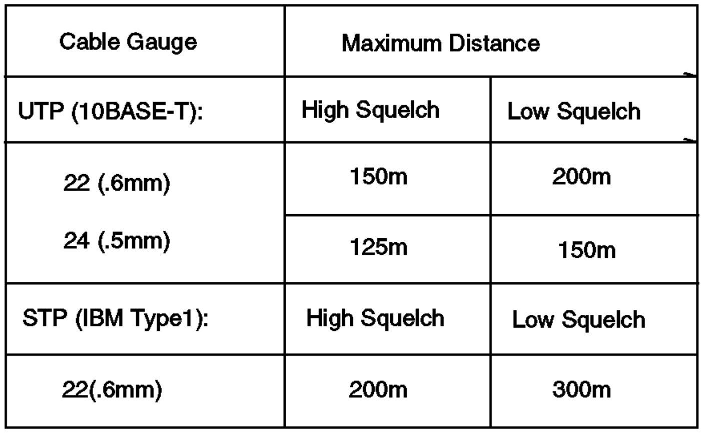
  You can enable/disable link Integrity for each port. To conform with the 10BASE-T standard, you should enable link integrity. But, to connect to older equipment which does not conform to the 10BASE-T standard, you may have to disable Link Integrity. You can use dip switches or the following management module command to perform this task:

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

  Note that link integrity must be enabled/disabled at both ends of the link or the module will report a link integrity error (one blink on the port status LED).

- Set squelch mode

Figure 72 on page 145 shows the maximum distances from the 10BASE-T module to a 10BASE-T transceiver (or another 10BASE-T module) for both shielded and unshielded twisted pair.



Cable Gauge	Maximum Distance	
UTP (10BASE-T):	High Squelch	Low Squelch
22 (.6mm)	150m	200m
24 (.5mm)	125m	150m
STP (IBM Type1):	High Squelch	Low Squelch
22(.6mm)	200m	300m

Figure 72. Maximum Distances with 10BASE-T Module

you can set the squelch mode to high (normal) or low (sensitive), using dip switches or the following management module command:

```
set port {slot.port} squelch {normal/low}
```

Low squelch mode will enable the module to receive a weaker signal, enabling you to increase achievable link distances by approximately 25% to 50%.

Setting squelch mode to low will result in added risk of losing packets to impulse noise on the unshielded twisted pair cables. But, setting the squelch level to low in conjunction with the IBM Type 1 cables increases the achievable link distance without sacrificing noise immunity.

Note that the squelch mode setting on the module should match the squelch mode setting on the 10BASE-T transceiver that it is connected to.

- Set crossover mode

  All eight ports on the 10BASE-T module are internally *crossed over* as per the 10BASE-T standard. This enables the 10BASE-T module to be connected directly to a 10BASE-T transceiver, for connecting to workstations.

  Port 8 can be *uncrossed* to allow the 10BASE-T module to be connected directly to another 10BASE-T module without the need for an external crossover adapter. Port 8 can be uncrossed, using the onboard dip switches or the following management module command:

  ```
  SET MODULE {slot} CROSSOVER {enable/disable}
  ```

  You may use 10BASE-T modules to connect two 8250s when the distance between the 8250s not exceed the maximum distance supported by the

10BASE-T modules. However, to achieve longer distances, we recommend that fiber modules be used for connecting 8250s.

When connecting two 10BASE-T modules, you must ensure that one port is crossed and the other port is uncrossed.

Note

The 10BASE-T module is 1/2 repeater; therefore, there can be no more than 8 10BASE-T modules on the signal path from one DTE to another.

7.5.4 Configuration Examples

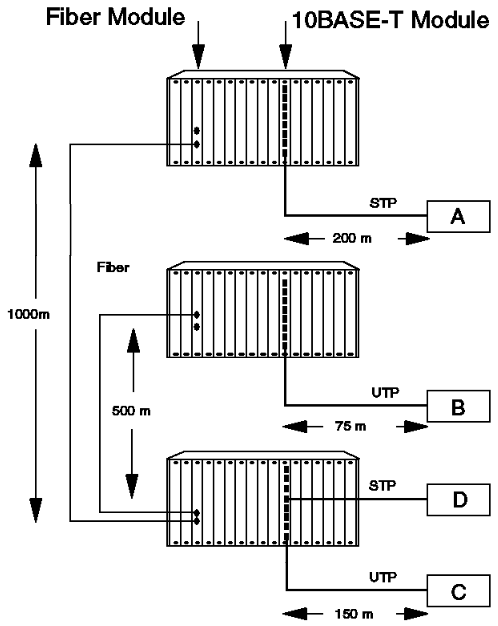


Figure 73. Fiber Backbone, Twisted Pair To-the-Desk

Figure 73 shows an example of a network design, where the fiber modules are used to provide backbone (8250-to-8250) connectivity, while the connectivity to the desk is provided via 10BASE-T modules.

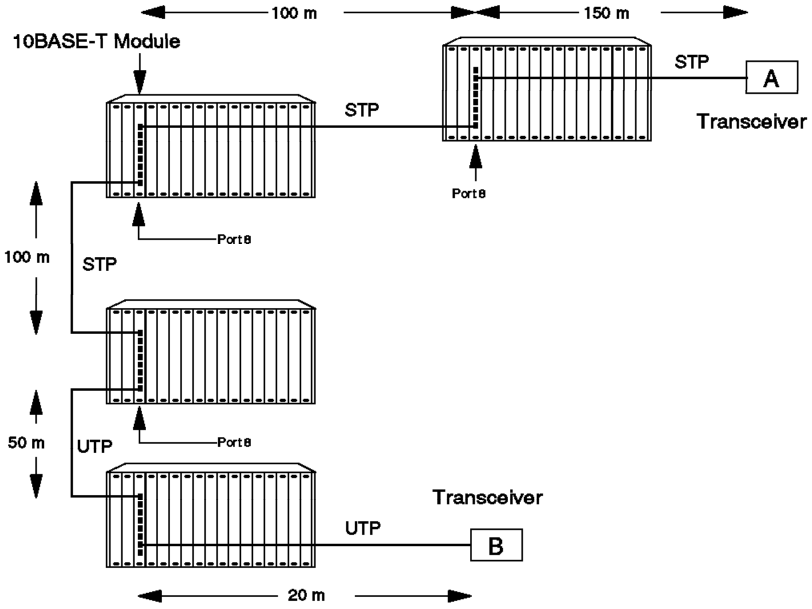


Figure 74. Twisted Pair Backbone, Twisted Pair To-the-Desk

Figure 74 is an example of using 10BASE-T modules to set up a network using twisted pair for both the backbone (8250-to-8250) and to-the-desk connectivity. Note that one end of the link between any two 8250s must be connected to port 8 on one of the concentrators to enable you to take advantage of the crossover mode setting available on the 10BASE-T modules.

7.5.5 Ethernet BNC Module

The Ethernet BNC module is a six-port *repeater* unit which allows a thin-wire (10BASE-2) segment to be attached to each of its ports. The repeater function provided by this module is fully compliant with the IEEE 802.3 standard and restores amplitude, phase and frequency of the signal received by the module. This will enable you to connect up to 6 thin-wire segments (each with 29 users) to your network which may consist of any of the other 8250 Ethernet modules.

Each thin-wire segment must be terminated with a 50 ohm termination at both ends. When the BNC module serves as the end-point to the segment, it can provide on board termination via dip switch settings without the need for an external terminator.

The BNC module can be assigned to any of the three Ethernet networks or can be isolated. All the ports will be switched to the network to which the module is assigned (this module does not have port-switching capability). The port assignment can be done via onboard dip switches or management module commands.

When the number of collisions, or duration of any collision, exceeds a threshold, the module automatically disables the port, and then enables the port when it again detects good data. This is called *automatic port portioning*.

Also, when a data packet which exceeds the legal Ethernet packet size is received, the module inserts gaps in the repeater output to prevent transceiver lockup.

The BNC module is one IEEE repeater. This should be taken into account because of the 4-repeater rule necessary in designing Ethernet networks.

Note

There can be a maximum of 12 BNC modules in an 8250 Model 017, while there is no restriction on the number which can be installed in a Model 006 or 6HC. This limitation is due to the power requirements of the BNC module.

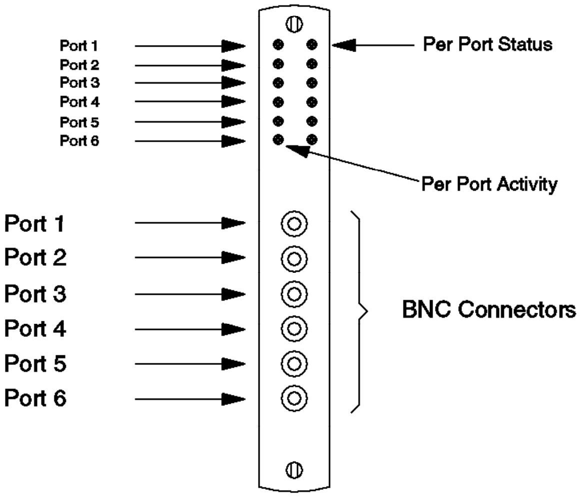


Figure 75. Front View of the BNC Module

The BNC module has 12 LEDs on the front panel that indicate the state of the ports. Figure 75 shows the locations of these indicators. The following table describes what these indicators mean.

Table 27. BNC Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Packets are being received on port from the segment.
		OFF	No activity on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		1 blink	Port partitioning.

Figure 76 on page 149 shows the BNC module′s dip switches, their meanings and the factory settings.

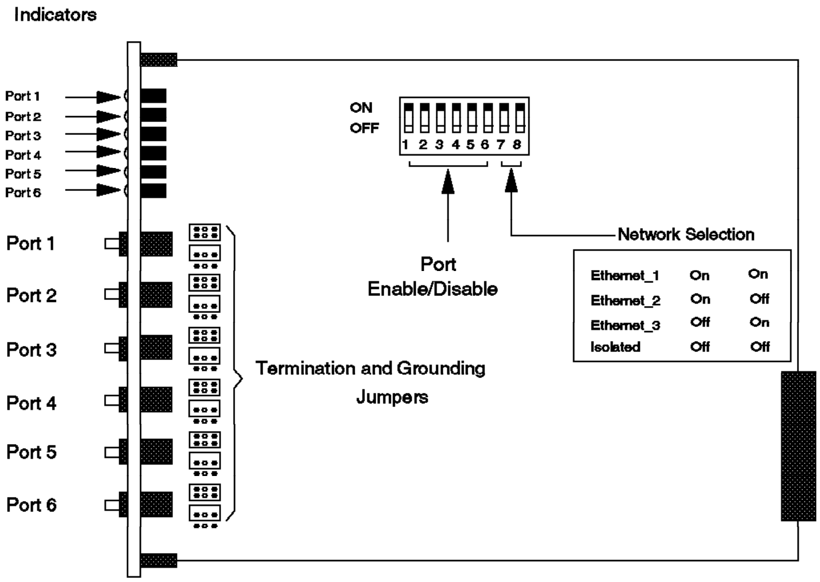


Figure 76. Side View of the BNC Module

7.5.6 Configuring Ethernet BNC Module

To configure the BNC module, you must do the following:

- Assign the module to a network

  The module can be assigned to Ethernet_1, Ethernet_2, Ethernet_3 or be isolated. This can be done via an onboard dip switch or through the following management module command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

- Enable/disable ports

  Each port can be enabled/disabled independently from the other ports. This can be done using onboard dip switches or the following management module command:

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

- Set termination and grounding jumpers

  The BNC module has twelve jumper locations for selection of termination and grounding for each port. Depending on your network configuration, you may be required to set one or more of these jumpers. For example, if the BNC module is serving as an end-point for a segment, the segment can be terminated through the termination jumper setting on that port. Also, as every segment must be grounded in one location, you could provide the grounding for a segment (if it is not already grounded) via the grounding jumper setting on that port.

  Note that jumper setting cannot be overridden via the management module commands.

  Figure 77 on page 150 shows the positioning and settings for these jumpers on the module.

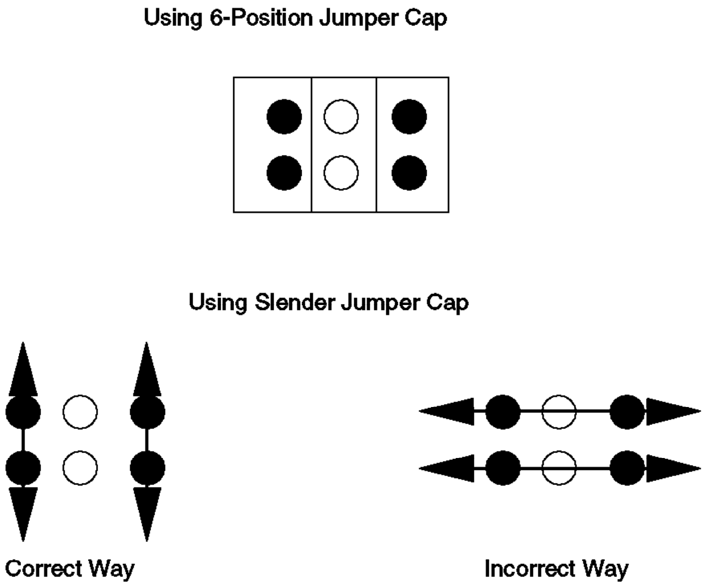


Figure 77. Jumper Setting for BNC Module

For proper grounding or termination, all four pins on a jumper block must be covered. Use a six-position jumper cap to cover the set of pins. If for any reason you must use two slender jumper caps in place of the six-position jumper cap, be sure to strap the pins vertically, not horizontally.

7.5.7 Configuration Example

Figure 78 on page 151 shows an example of using a BNC module. Two thin-wire segments are connected to two ports on the BNC module, enabling the workstations on these two segments to communicate with each other.

One of the two segments is externally terminated at both ends; therefore, the BNC port which is connected to that segment should have the termination jumper removed. In the other segment, where the BNC port serves as the end point on the segment, the termination can be provided via jumper setting on the BNC port.

Note

The dotted line in this diagram means that the BNC T-connector is directly attached to the hub port and there is no cable involved.

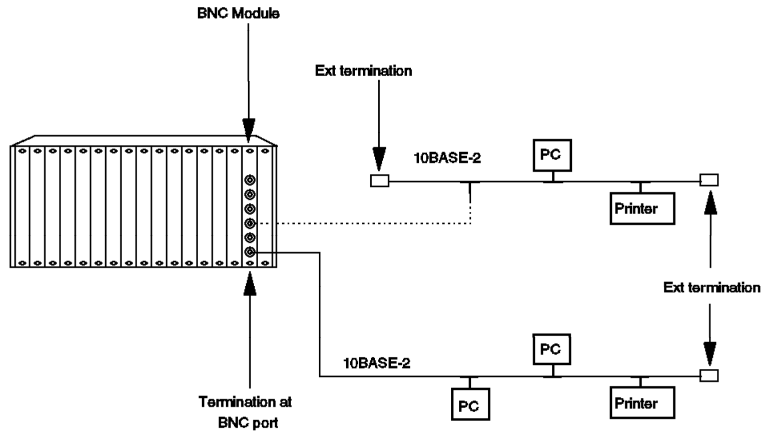


Figure 78. Configuration Example

Note that if this BNC module is connected to a network which has other Ethernet modules connected to it, the workstations on these two segments will be able to communicate with the workstations attached to those modules as well.

7.6 10BASE-T TELCO Modules

The 10BASE-T TELCO modules provide IEEE 802.3 repeater ports that comply with the 10BASE-T standard. These modules have 50-pin TELCO connectors which can be used to connect to an external 12-port *harmonica*. Each port on the harmonica provides an RJ-45 connector for attaching 10BASE-T compliant DTEs.

The 50-pin TELCO modules are available in three models:

- 10BASE-T, 12-port, TELCO, UTP
- 10BASE-T, 12-port TELCO, UTP with port switching
- 10BASE-T, 24-port TELCO UTP with bank switching

The port-switching capability allows you to connect any of the ports to Ethernet_1, Ethernet_2, Ethernet_3 or isolated mode. To perform port switching, a management module must be installed in the 8250.

The 24-Port, bank-switching module has two 50 pin TELCO connectors each supporting 12 UTP ports. The bank switching capability allows you to assign either of the *banks* of 12 ports to Ethernet_1, Ethernet_2, Ethernet_3 or isolated mode. To perform bank-switching a management module must be installed in the 8250.

The distances achievable using UTP with the 50-Pin module are:

- 150 m on 22 gauge wire

- 125 m on 24 gauge wire

Note

Unlike the 10BASE-T module, the 50-pin modules do not support connections using shielded twisted pairs.

In conformance with the 10BASE-T standard, all ports are internally crossed over which allows you to connect them directly to 10BASE-T transceivers without using external crossover adapters.

Although not recommended, because of limited achievable distances, the 50-pin modules can also be used to provide a UTP backbone connecting two or more 8250s together. In this case, an external crossover adapter is required.

In addition, this module provides support for features that are beyond the scope of the 10BASE-T standard. These are:

- Allow you to set low *squelch* level which increases the achievable distances (given above) by 25% to 50%.
- Allow *link integrity* to be disabled for communication with older equipment.
- Allow *receive jabber* to be enabled which will prevent an uncontrolled jabber condition.

A 10BASE-T TELCO module consists of a repeater and twisted pair transceivers. Incoming signals received on the twisted pair link are regenerated so that the amplitude, phase, and frequency are restored. The repeated signal is synchronized to the system clock and put on the backplane. Outgoing signals from the backplane are sent directly to be transmitted on the twisted pair segments.

Note

A 50-pin TELCO module is 1/2 repeater.

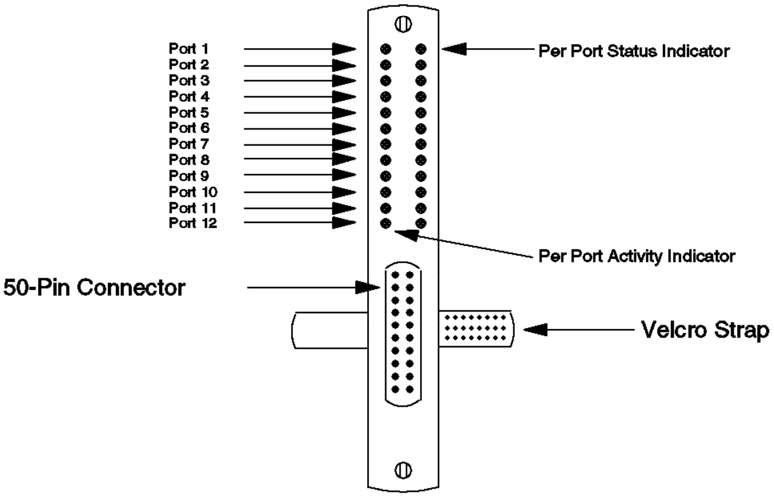


Figure 79. Front View of 12-Port TELCO Module

The 12-port TELCO module has 24 LEDs on the front panel that indicate the state of the ports. Figure 79 shows the locations of these indicators. The following table describes what these indicators mean.

Table 28. 10BASE-T 12-Port TELCO Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the segment.
		OFF	No activity on the segment.
		Blinking	Packets are received on the segment.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		1 blink	Link failure.
		2 blinks	Port partitioned.
		6 blinks	Receive jabber.

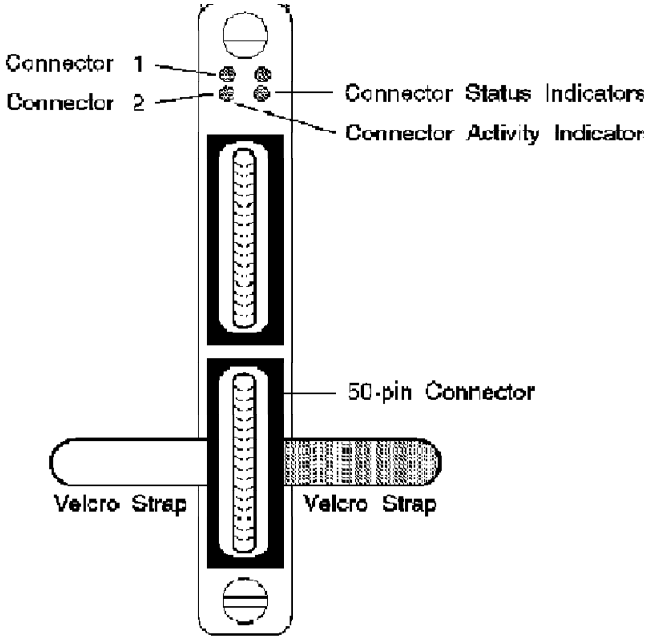
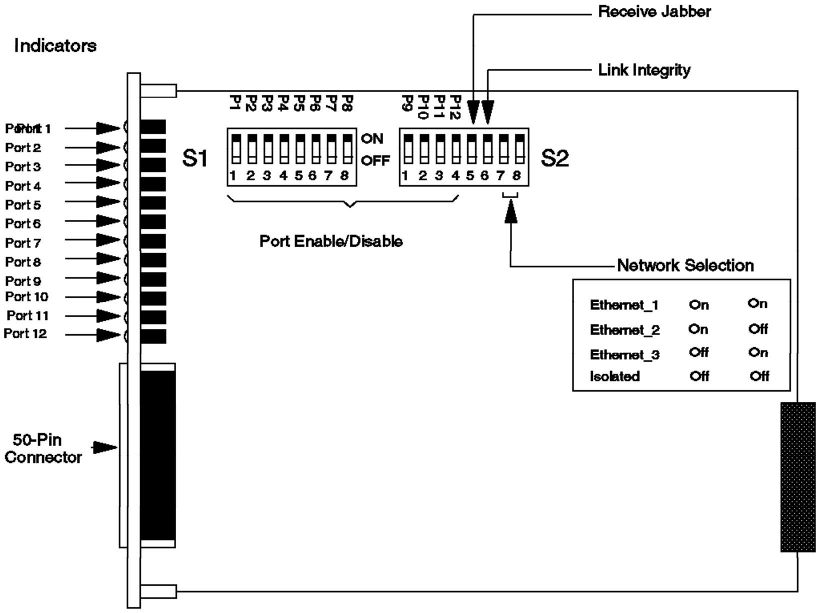


Figure 80. Front View of 24-port TELCO Module

The 24-port TELCO module has 4 LEDs on the front panel that indicate the state of the ports. Figure 80 shows the location of these indicators. The following table describes what these indicators mean.

Table 29. 10BASE-T 24-Port TELCO Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Constant activity on the connector.
		OFF	No activity on the connector.
		Blinking	Packets are received on the connector.
Status	Green	ON	Connector enabled.
		OFF	Connector disabled.
		1 blink	Link failure.
		2 blinks	Port partitioned.



Ethernet_1	On	On
Ethernet_2	On	Off
Ethernet_3	Off	On
Isolated	Off	Off

Figure 81. Side View of the 12-port TELCO Module

Figure 81 shows a side view of the 12-Port TELCO module, its dip switches, their meanings and their factory settings.

7.6.1 Configuring Ethernet 10BASE-T TELCO Module

To configure the 50-Pin TELCO module you must do the following:

- Assign the module/port/bank to a network

  Depending on the type of 50-pin TELCO module, you could assign the *module*, the individual *ports* or the *bank* of ports to Ethernet_1, Ethernet_2, Ethernet_3 or isolated mode. Individual *ports* are assignable in the case of the 12-port TELCO module with port-switching only, and the *bank* of ports are assignable in the case of the 24-port TELCO module only.

  To effect *port* or *bank* switching, a management module must be installed in the 8250.

  The module assignment can be done via onboard dip switches or the management module commands.

  The management module commands used for each case are:

  – Assign a module to a network:

    SET MODULE {slot} NETWORK {network}

  – Assign a port to a network (port-switching model only)

    SET PORT {slot.port} NETWORK {network}

  – Assign a bank of ports to a network (bank-switching model only)

    SET BANK {slot.bank} NETWORK {network}

- Enable/disable ports

  Each port on the 50-pin TELCO modules can be enabled/disabled independently from the other ports. This can be done via onboard dip switches or the following management module command:

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

- Enable/disable link integrity

  To conform with the 10BASE-T standard, link integrity should be enabled. But, to connect to some older equipment which does not conform to the 10BASE-T standard, you may have to disable link integrity. This can be done via onboard dip switches or the following management module command:

  ```
  SET PORT {slot.port} MODE LINK_INTEGRITY {enable/disable}
  ```

  Using dip switches allows you to enable/disable link integrity for the module only, while using the management module command will allow you to enable/disable link integrity for individual ports.

  Note that link integrity must be enabled/disabled at both ends of the link or the module will report a link integrity error (one blink on the port status LED).

- Set squelch mode

  You can set the squelch mode to *High* (normal) or *Low* (sensitive). *Low* squelch mode will enable the module to receive a weaker signal on that port, enabling you to increase achievable link distances by approximately 25% to 50%. To set the squelch mode, you must use the following management module command:

  ```
  SET PORT {slot.port} SQUELCH {normal/low}
  ```

  There are no dip switches for setting the squelch mode.

  Setting squelch mode to low will result in added risk of losing packets to impulse noise on the unshielded twisted pair cables, which is the only type of cable supported by the 50-pin TELCO modules.

  Note that squelch mode setting on the module should match the squelch mode setting on the 10BASE-T transceiver to which it is connected.

- Set receive jabber mode

  If a jabber condition occurs for one of the attached DTEs, the transceiver attached to that DTE is responsible for protecting the network from the jabber condition. However, to protect the network in case the transceiver fails to halt a jabbering DTE, the 50-pin TELCO module provides you with a facility to enable *receive jabber* mode. This provides the highest degree of jabber protection by disconnecting the jabbering DTE 10 microseconds after the jabber is received by the 50-pin TELCO module. Note that this facility is not part of the 10BASE-T standard.

  You can enable/disable *receive jabber* for the whole module via an onboard dip switch. Through the following management module command you can set receive jabber mode for individual ports:

  ```
  SET PORT {slot.port} RECEIVE_JABBER {enable/disable}
  ```

- Enable/disable port redundancy

  You can enable/disable link redundancy between ports on the 50-pin TELCO module to provide backup in one of the following cases:

  - Link failure
  - Port failure
  - Port partition
  - Jabber condition

Note that when you enable port redundancy, the setting of port enable/disable switches for these ports is ignored. You must also ensure that port redundancy is set at one end of the link only, to prevent unpredictable results. Port redundancy can only be set if a management module is installed in the 8250. The format of the command is as follows:

```
SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}
```

Port redundancy can be between two ports on the same module or between the ports across different modules installed on the same 8250. The latter requires an advanced management module to be installed in the 8250.

7.6.2 Configuration Examples

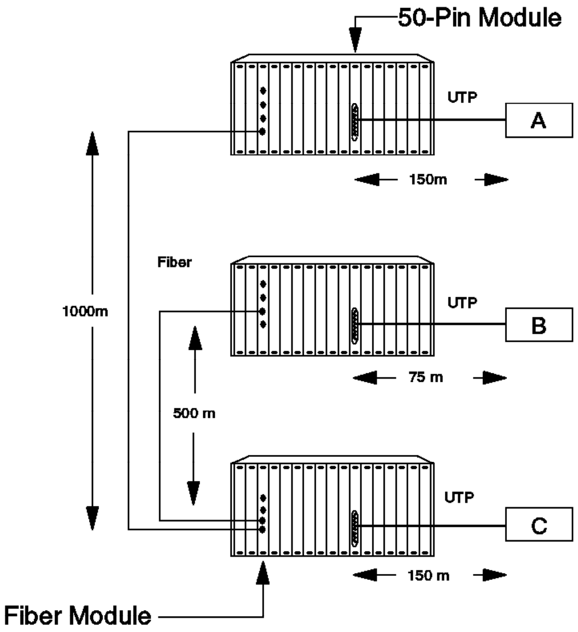


Figure 82. Using 50-Pin TELCO Module with Fiber Backbone

Figure 82 is an example of a network design, where the fiber modules are used to provide backbone (8250-to-8250) connectivity, while the connectivity to the desk is provided via 50-pin TELCO modules.

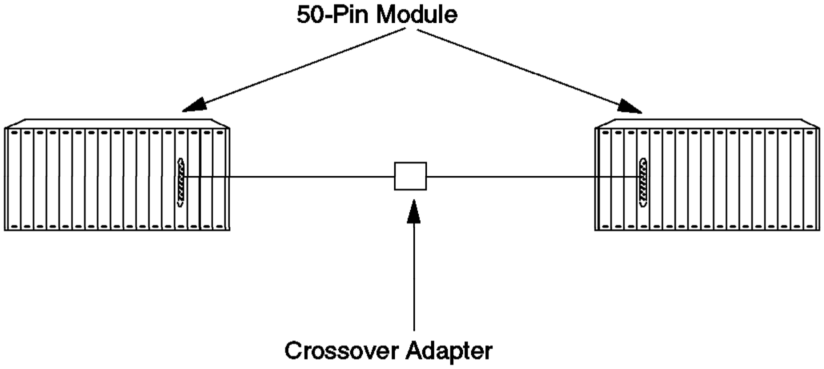


Figure 83. Twisted Pair Backbone Using 50-Pin Module

Figure 83 shows an example of using 50-pin modules to set up a network using twisted pair for the backbone (8250-to-8250). As the ports are internally crossed (in conformance with the 10BASE-T standard) you will need to use an external *crossover adapter* to make the connection between the two 8250s.

Note: We recommend that you use fiber cable for backbones as it permits longer distances between concentrators.

7.7 Ethernet Transceiver Module

The Ethernet transceiver module is a three-port IEEE 802.3 compatible transceiver which allows connection of *workstations*, *repeaters*, *routers* and *bridges* directly to the 8250 via an AUI cable. This allows you to connect an existing network to the 8250 via external repeaters, routers or bridges.

Any of the ports on the transceiver module can be enabled/disabled independently and assigned to any of the three Ethernet networks or be isolated. The port assignment can be done via onboard dip switches or management module commands.

You can also provide redundancy between any two ports via an onboard dip switch or through a management module command. This allows you to provide backup for a connection in case of link or port failure.

To provide compatibility with IEEE repeaters, you can enable/disable SQE test mode for each port.

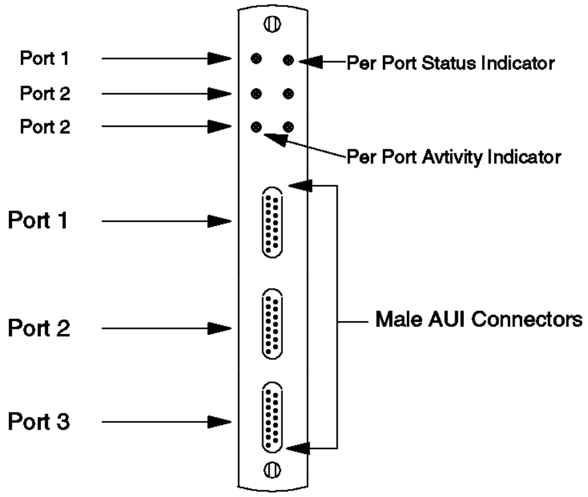


Figure 84. Front View of the Transceiver Module

The transceiver module has 6 LEDs on the front panel that indicate the state of the ports. (There is no LED indicator for port redundancy.) Figure 84 shows the location of these indicators. The following table describes what these indicators mean.

Table 30. Transceiver Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Packets are received from the attached device.
		OFF	No packets are received from the attached device.
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		1 blink	No AUI DC power from the device connected to this port.
		2 blinks	Attached device is jabbering.

Figure 85 on page 160 shows the transceiver module side view, its dip switches, their meanings and factory settings.

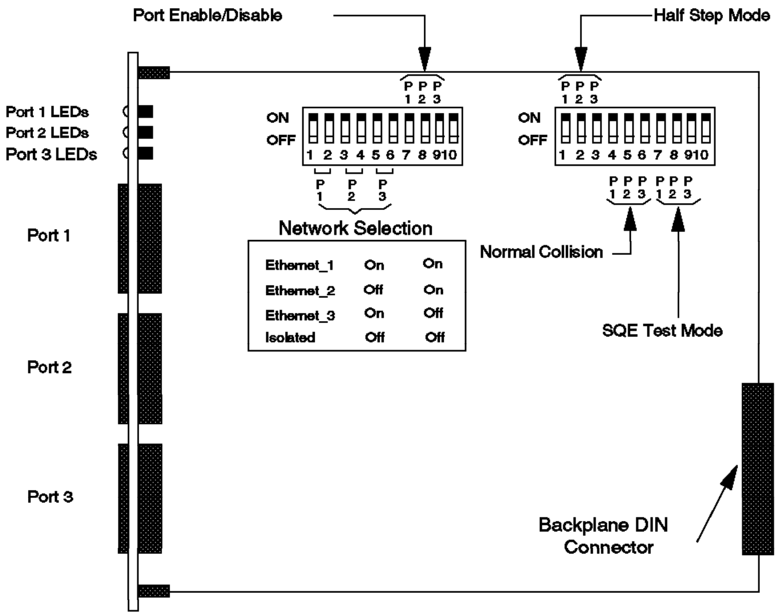


Figure 85. Side View of the Transceiver Module

7.7.1 Configuring Ethernet Transceiver Module

To configure the transceiver module, you must do the following:

- Assign each port to a network

  Each port can be assigned to Ethernet_1, Ethernet_2, Ethernet_3 or be isolated. This can be done via an onboard dip switches or through the following management module command:

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

- Enable/disable ports

  Each port can be enabled/disabled independently from the other ports. This can be done via onboard dip switches or the following management module command:

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

- Set redundancy mode between ports

  You may choose to provide redundancy between any two ports on the module. This can only be done through the use of management module commands. There is no dip switch onboard the module for setting redundancy mode. The format of the management module command is as follows:

  ```
  SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}
  ```

  In redundancy mode, the switch-over to the backup link will take place automatically in case of primary port or link failure. The link switches back automatically once the primary port recovers. When the primary link is operating satisfactorily, the backup link will carry no traffic.

- Disable SQE test mode on the transceiver

In compliance with the IEEE standard, the transceiver module provides a Signal Quality Error (SQE) test option which enables the transceiver to test the collision detection capability on the DTEs by asserting collision at the end of each packet which is transmitted. IEEE repeaters interpret this as a collisions and will subsequently partition that port. Therefore, if SQE test mode is enabled on the transceiver module ports that are connected to a repeater, severe network degradation will result. You must ensure that any port connected to a repeater has SQE test mode disabled.

For the transceiver module, the SQE test mode can be enabled/disabled for each port via the onboard dip switches or the following management module command:

```
SET PORT {slot.port} SQE_TEST {enable/disable}
```

Note

Certain non-IEEE 802.3 repeaters require the SQE test mode to be enabled.

- Set half/full step mode

  All IEEE 802.3 and Ethernet Version 2.0 devices use *half-step* signalling on the AUI cable, but some pre-Version 2.0 Ethernet devices require the use of *full-step* signalling.

  The transceiver module comes with all ports factory set to half-step signalling mode. This can be changed via onboard dip switches or the following management module command to full-step mode when connecting to pre-Version 2.0 Ethernet devices:

  ```
  SET PORT {slot.port} HALF_STEP {enable/disable}
  ```

- Set normal/alternate collision mode

  IEEE 802.3 requires the *normal collision* mode which results in collisions being signalled to AUI for as long as they last on the medium.

  All the ports on the transceiver module are factory set to operate at normal collision mode. But, each port can be set independently, via onboard dip switches or the following management module command, to operate in *alternate collision* mode which is required when the 8250 communicates with certain controller chips which are not compliant with IEEE specifications:

  ```
  SET PORT {slot.port} COLLISION {normal/alternate}
  ```

7.7.2 Configuration Example

Figure 86 on page 162 shows that by using transceiver and fiber modules, we can connect several different networks together, so that the users on those networks can communicate with each other to exchange information and share resources.

Note that in this configuration, an end-node is connected to one of the transceiver modules via an AUI cable. The 8250 and its modules can be configured so that this node can communicate with all the stations on the shown thick and thin-Coax Ethernet networks.

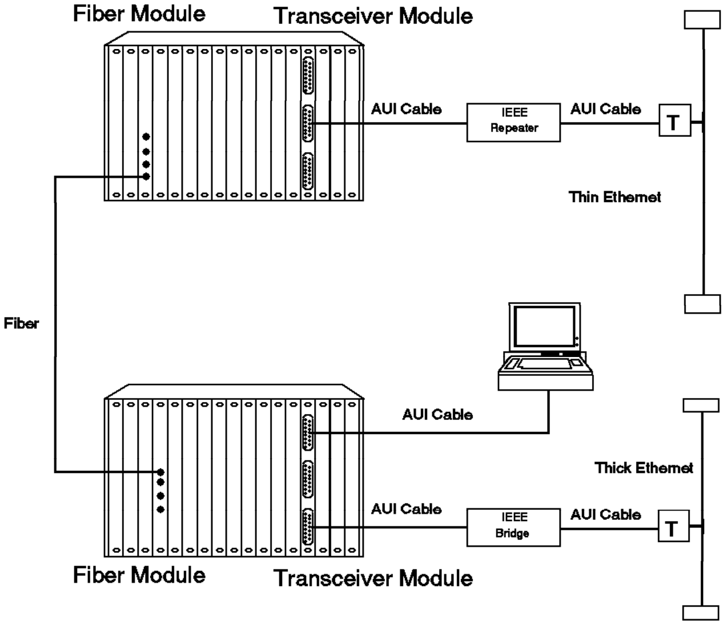


Figure 86. Configuration Example

7.7.3 Ethernet Repeater Module

The Ethernet repeater module is a two-port repeater unit which allows for the direct connection of up to two Ethernet segments to the IBM 8250 Multiprotocol Intelligent Hub, via an AUI cable and external transceivers. The repeater module provides the means for connecting Ethernet segments running on different media types (such as thick coax or thin coax) to the IBM 8250. Either port can connect to any media type, allowing you to extend your network by connecting Ethernet segments running on different media types.

The repeater function which is provided with this module is fully compliant with the IEEE 802.3 standard (restores amplitude, phase and frequency of the signal).

Each port on the repeater module can be assigned to any of the three Ethernet networks or can be isolated. The port assignment can be done via onboard dip switches or the management module commands.

When the ports are isolated, the workstations on the segments connected to these two ports can communicate only with each other. This allows you to connect two segments without occupying one of the Ethernet networks on the backplane.

You can also provide redundancy between the two ports via an onboard dip switch or through a management module command. This allows you to provide backup for a connection in case of link or port failure.

Port redundancy provided by the repeater module can be used to provide two connections (one primary and one backup) from an Ethernet segment to the 8250. This can be used to ensure that the connection between the segment and the 8250 will be maintained in case one of the connections fails. Figure 89 on page 166 shows an example of this type of configuration.

When the number of collisions, or duration of any collision exceeds a threshold, the repeater module automatically disables the port, and then enables the port when it again detects good data. This is called *automatic port partitioning*.

Also, when a data packet which exceeds the legal Ethernet packet size is received, the module inserts gaps in the repeater output to prevent transceiver lockup.

Note

The repeater module uses significantly more power than other modules. Therefore, there is a limit on the number of repeater modules which can be installed on an 8250. The numbers are:

- Maximum of 6 repeater modules per 8250 Model 017
- Maximum of 2 repeater modules per 8250 Model 006 and 6HC

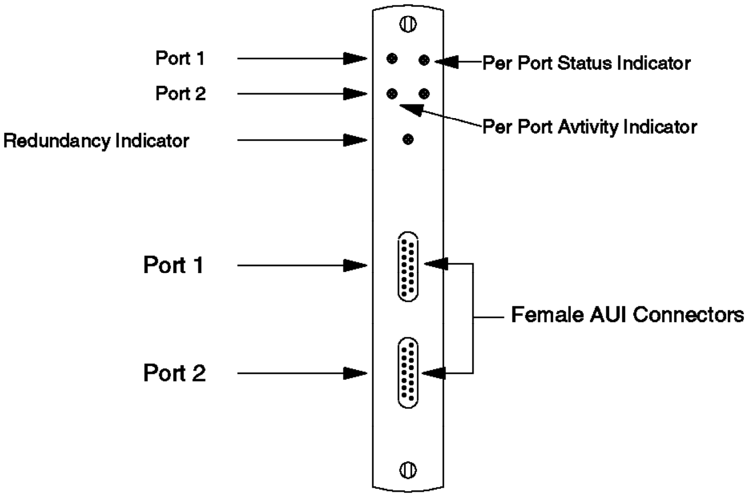


Figure 87. Front View of the Repeater Module

The repeater module has 5 LEDs on the front panel that indicate the state of the ports and port redundancy. Figure 87 shows the location of these indicators. The following table describes what these indicators means.

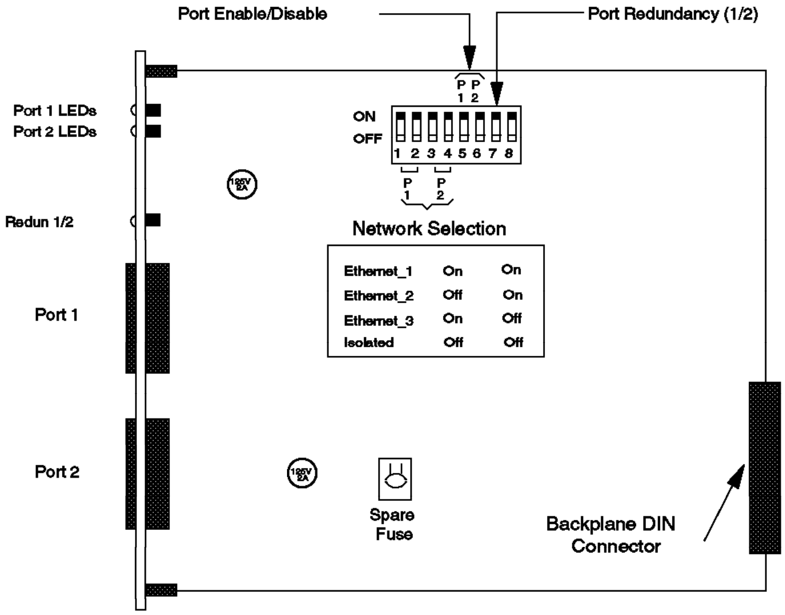
Table 31 (Page 1 of 2). Repeater Module LED Descriptions

LED name	Color	State	Description
Activity	Yellow	ON	Packets are received from the segment.
		OFF	No packets are received segment.

Table 31 (Page 2 of 2). Repeater Module LED Descriptions

LED name	Color	State	Description
Status	Green	ON	Port enabled.
		OFF	Port disabled.
		1 blink	Carrier loss.
		2 blinks	Port partitioning.
Redundancy	Green	ON	Redundancy enabled between ports 1/2.
		OFF	Redundancy disabled.
		Blinking	Connection has been switched to the backup link.

Figure 88 shows the side view of the repeater module, its dip switches, their meanings and the factory settings.



Network Selection

Ethernet_1	On	On
Ethernet_2	Off	On
Ethernet_3	On	Off
Isolated	Off	Off

Figure 88. Side View of the Repeater Module

Note

Due to large in-rush current, certain transceivers, particularly the older ones are prone to blowing fuses on the attached devices. Therefore, the repeater module is equipped with two 2 Amp fuses to protect its circuitry when operating with such transceivers. Also, a spare fuse is provided if one of those two fuses is blown. To replace the fuse, the repeater module must be removed from the concentrator.

7.7.4 Configuring Ethernet Repeater Module

To configure the repeater module, you must do the following:

- Assign each port to a network

  SET MODULE {slot} NETWORK {network}

  Each port can be assigned to Ethernet_1, Ethernet_2, Ethernet_3 or isolated. This can be done via onboard dip switches or through the following management module command:

  SET MODULE {slot} NETWORK {network}

- Enable/disable any of the 2 ports

  Each port can be enabled/disabled independently from the other ports. This can be done using onboard dip switches or through the following management module command:

  SET PORT {slot.port} MODE {enable/disable}

- Set redundancy mode for port 1 and 2

  You may set one of the ports as redundant for the other. In this case, the switch-over to the backup link will take place automatically in case of primary port or link failure. When the primary link is operating satisfactorily, the backup link will carry no traffic.

  Port redundancy can be set via the onboard dip switches or the following management module command:

  SET PORT {slot.port} MODE {redundant/non_redundant} {slot.port}

- Disable SQE test mode on the attached transceiver

  To connect the repeater module to an Ethernet segment, a transceiver is required. All the IEEE transceivers provide a Signal Quality Error (SQE) test option. As mentioned earlier, if SQE test mode is enabled on any transceiver connected to either port of the repeater module, severe network degradation will result. Therefore, you must ensure that SQE test mode is disabled on the transceivers attached to the repeater module ports.

7.7.5 Configuration Example

Figure 89 on page 166 shows that by using repeater and fiber modules you can connect several different networks between buildings, so that the users on those networks can communicate with each other to exchange information and share resources.

Note that in connecting to one of the networks (thick coax network), we have taken advantage of the *port redundancy* facility offered by the repeater module to ensure that in case of a link or port failure, the connection to that network will still be available through the backup link.

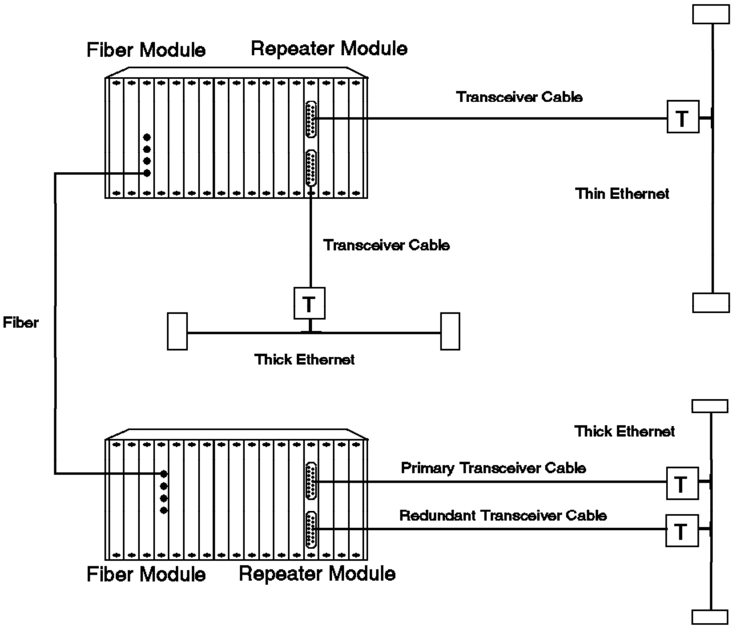


Figure 89. Configuration Example

7.8 Ethernet Bridge Module

The Ethernet bridge module is a high-performance *transparent bridge* that allows you to connect Ethernet V2.0 and/or IEEE 802.3 networks together to form a single extended LAN.

The bridge module fits into the 8250 and occupies *two* slots on the concentrator. It provides connections for the two LANs to be bridged. One of the connections can be through the female AUI port provided on the bridge module or through the backplane, while the other connection is always over the backplane. The decision to use one external and one backplane connection (or two backplane connections) for the bridge is determined via onboard dip switches or a management module command, or via a bridge command entered through an ASCII terminal directly connected to the RS-232 port provided on the bridge module.

This ability to connect the bridge to any two 8250 backplane Ethernet networks (or one 8250 backplane Ethernet network and one external connection) will allow you to change the LAN topology, remotely, using the facilities offered by the bridge management facilities or a management module command.

When attached to a network, the bridge module will automatically learn the addresses of all the stations on that network. This is done by storing the source address of each packet generated on that network in a database on the bridge module.

The Ethernet bridge module is a high-performance bridge which uses a high-speed multi-port memory so that the IEEE 802.3 stations and the CPU all have separate access to the common packet memory. This allows the bridge to forward up to 10,000 packets per second.

Filtering can be used to stop the forwarding of unwanted traffic over the bridge. The bridge module uses dedicated hardware to accelerate the address filtering operation to ensure the highest possible performance in the bridge. The filtering facility provided by the bridge module allows you to filter or forward the packets based on their destination address and/or protocol type they use.

The bridge module supports a spanning tree protocol which ensures that only one bridge enters *data forwarding* mode when there is more than one bridge installed between the two LANs. In this case, the other bridges will be in *blocking mode*. If the data forwarding bridge fails, the spanning tree protocol will ensure that one of the bridges in blocking mode will take over the responsibility of forwarding data, automatically.

The bridge module can be managed via an ASCII terminal connected to the RS-232 port on the bridge module. You can also access the module through an in-band connection from another bridge module or an Ethernet management module using the *remote-logon* facility offered by the Ethernet bridge modules and Ethernet management modules. The bridge module also provides SNMP support which allows the bridge to be managed via AIX NetView Hub Management Program/6000.

New firmware can be downloaded to the bridge module via a PC attached to the bridge module′s RS-232 port. This connection can be either a direct attachment or through a modem-attached communication line.

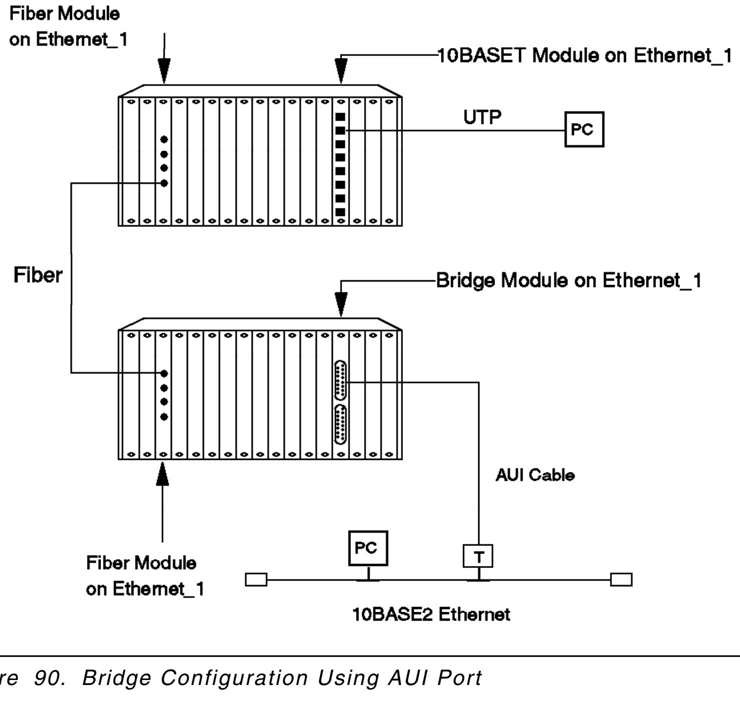

Fiber Module on Ethernet_1
10BASET Module on Ethernet_1
UTP
PC
Fiber
Bridge Module on Ethernet_1
AUI Cable
PC
T
Fiber Module on Ethernet_1
10BASE2 Ethernet

Figure 90. Bridge Configuration Using AUI Port

As mentioned before, the bridge module has two connection alternatives:

1. One AUI port connector (port 1) and one backplane connector (port 2)
2. Two backplane connectors (ports 1 and 2)

Figure 90 shows the use of the first alternative, where an external network is connected to the AUI port and the other network is connected to the bridge module via one of the backplane networks. Note that the AUI port is a female connector which can be connected to a transceiver using an AUI cable.

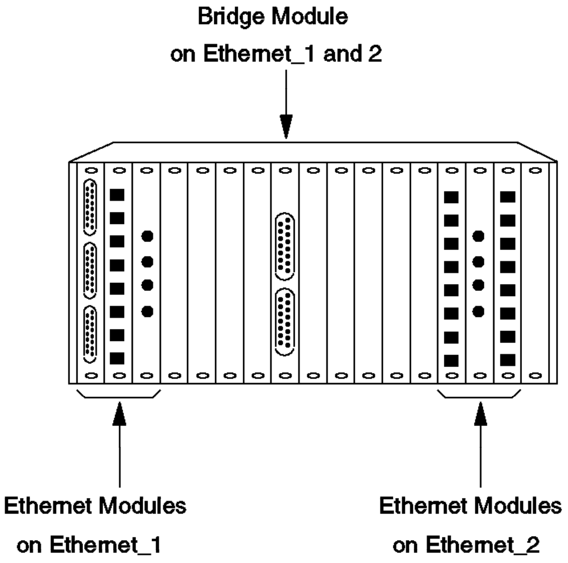


Figure 91. Bridge Configuration Using Backplane

Figure 91 shows the use of two backplane connections by the bridge module to bridge two backplane networks. In this example, Ethernet_1 is bridged to Ethernet_2. Note that any two Ethernet networks can be bridged in this way.

In this type of connection, port 1 on the bridge module can be connected to Ethernet_1, Ethernet_2 or isolated, while port 2 can be connected to any of the three ETHERNET networks or isolated. However, the use of *isolated* mode for any of the bridge ports will result in the other port being bridged to nothing.

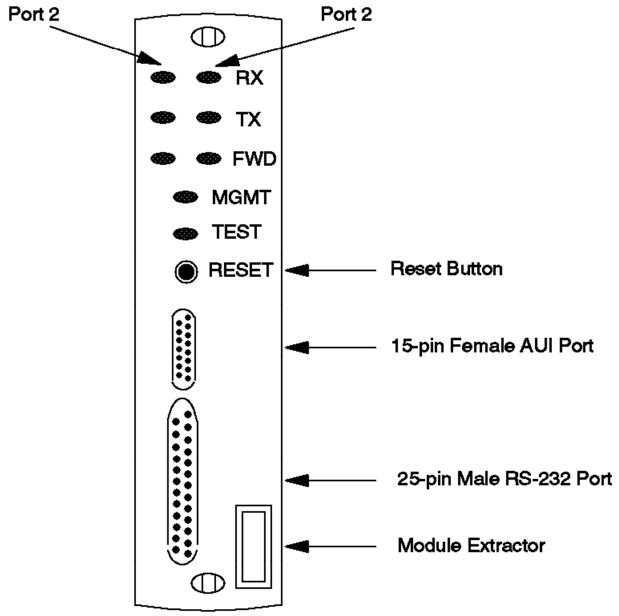


Figure 92. Front View of the Bridge Module

Figure 92 shows a front view of the bridge module. As can be seen, the bridge module has 8 LEDs on the front panel that indicate the state of the ports. There is also a *reset button* which allows you to reset the module. Pressing this button has the same effect as entering the bridge′s *reset* command. The effect of resetting the bridge module will be discussed later.

The *module extractor* is for easy removal of the module from the 8250.

The RS-232 port is for connecting a terminal or PC to manage the bridge module directly via an ASCII terminal.

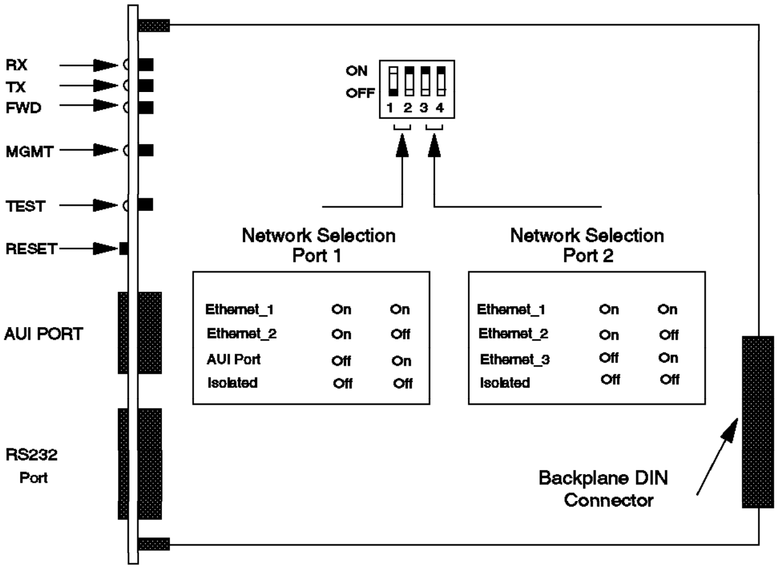
The AUI port is for external network connection.

The following table describes the normal meanings of the LEDs.

Table 32. Bridge Module LEDs

LED	Function
RX	Indicates receive activity on the network connected to this port.
TX	Indicates transmit activity on the network connected to this port.
FWD	Indicates the bridge is in forwarding state.
MGMT	Indicates the administrator mode of the bridge is active.
TEST	Indicates the Bridge Module Self-Test activity.

Figure 93 on page 170 shows the bridge module dip switches, their meanings and the factory settings.



Network Selection
Port 1

Ethernet_1	On	On
Ethernet_2	On	Off
AUI Port	Off	On
Isolated	Off	Off

Network Selection
Port 2

Ethernet_1	On	On
Ethernet_2	On	Off
Ethernet_3	Off	On
Isolated	Off	Off

Figure 93. Side View of the Bridge Module

7.8.1 Topology Switching Using Bridge Module

Figure 94 shows how the internal *multi-switch* (B) residing in the bridge module allows you to bridge the AUI port to any backplane network or to bridge any two backplane networks.

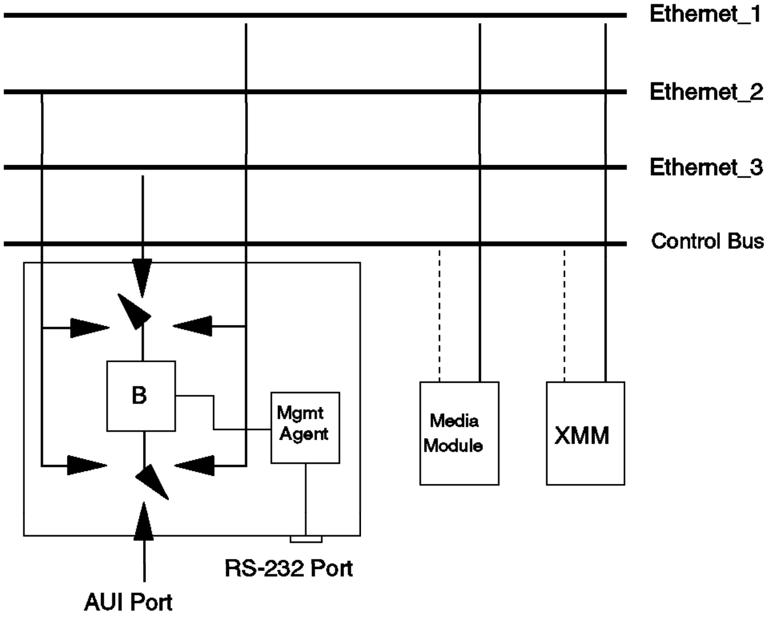


Figure 94. Topology Switching

The switching of the bridge module to a network can be done (out-of-band) using the RS-232 port provided on the bridge module or (in-band) using a management module or AIX NetView Hub Management Program/6000.

Note

Port 1 on the bridge can only be connected to Ethernet_1, 2, or isolated while port 2 can be connected to Ethernet_1, 2, 3, or isolated. This is because one set of dip switch settings for port 1 is used to indicate that an AUI port is used instead of one of the backplane connections.

7.8.2 Configuring Ethernet Bridge Module

Before using the bridge module you must do the following:

7.8.2.1 Connect a Terminal to the Bridge Module

The bridge module is accessed through the RS-232 port on the front of the module. You can connect any device that presents an ASCII interface, such as ASCII terminals or PCs with ASCII terminal emulation.

You need to make sure that the terminal is initially configured with exactly the same parameters that are set as default for the bridge module. The following parameters are required to be set for the terminal:

```
Baud          9600
Data bits     8
Parity        NONE
Stop bits     2
```

After you have configured your terminal to match the factory defaults of the bridge module, the terminal can be connected to the RS-232 port on the bridge module. You may then use the following command to change the terminal characteristics required by the bridge module:

```
SET TERMINAL parameters
```

The following parameters can be specified in the *set terminal* command:

```
BAUD       {300, 1200, 2400, or 9600}
DATA_BITS  {7 or 8}
HANGUP     {enable or disable}
PARITY     {even, odd, or none}
PROMPT     {new prompt up to 15 characters}
STOP_BITS  {1 or 2}
TIMEOUT    {0 - 30}
```

After changing the above parameters, you must issue *save terminal* command to save the new values.

Note

When you change the *baud*, *data_bits*, or *parity* parameters, you immediately lose your connection to the terminal. Therefore, you must change the corresponding value on the terminal and then press the *Enter* key to return to the bridge module prompt and then save the terminal settings.

7.8.2.2 Set SNMP parameters

If you are planning to use an SNMP station such as AIX NetView Hub Management Program/6000 to manage the bridge module, you must set the following parameters:

- Set IP address for the bridge module

  SNMP requires the use of TCP/IP which in turn requires each device on the network to have a unique IP address. Use the *set device ip_address* command to assign a unique IP address to each port of your bridge module. The format of the command is as follows:

  ```
  SET DEVICE IP_ADDRESS PORTn xx.xx.xx.xx
  ```

- Set community table

  Community table defines which SNMP stations can *query* and/or *set* the parameters in your bridge module, and which station(s) will receive *traps* generated by the bridge module. Use the *set community* command to set up the community table. The format of the command is as follows:

  ```
  SET COMMUNITY nnnn xx.xx.xx.xx {access variable}
  ```

  where *nnnn* is the name of the SNMP station to be added to the community table and the *access variables* can be *trap*, *read_write*, *read_trap*, *read_only*, or *all*.

- Set default gateway

  Default gateway specifies the IP address of the *gateway* to which the bridge module should forward its SNMP packets whose destination address is not known in the local network. Use the *set device* command to specify a default gateway for each port on your bridge module.

  ```
  SET DEVICE DEFAULT GATEWAY PORTn xx.xx.xx.xx
  ```

- Set subnetwork mask

  Use the *set device* command to set the *subnet mask* for each port on the bridge module.

  ```
  SET DEVICE SUBNET_MASK PORTn xx.xx.xx.xx
  ```

  More information about subnetwork mask can be found in 4.3, "IP Subnets" on page 76.

- Set alert settings

  The *set alert* command is used to enable or disable sending of various *alerts* to the SNMP manager. The *alert* types which can be enabled/disabled are:

  - *Authentication* - If a user, who is not listed in the community table with the proper access, tries to access the bridge module, a trap will be sent to the SNMP manager(s) who is(are) specified as *trap receiver(s)* in the bridge module′s community table.

  - *Change* - Allows the bridge module to send traps every time a change is made to its configuration.

  - *Hello* - Allows a bridge module to send a trap after it is *Reset*. The trap is sent once every minute (for up to 255 times) until the SNMP manager acknowledges the bridge module. If after 255 traps, no acknowledgment is received, the bridge module will stop sending the *hello traps*.

  Use the *set alert* command to change the *alert* settings.

```
SET ALERT HELLO  disable
SET ALERT CHANGE enable
SET ALERT AUTHENTICATION enable
```

7.8.2.3 Set Filtering Attributes

For performance and security reasons, you should ensure that only the desired traffic is forwarded by the bridge module. This can be done by setting the bridge module′s *filters* before connecting it to the networks.

Use the *set filter* command from the terminal to specify the *address* and *protocol-id* filtering attributes. This allows you to set up criteria for filtering and/or forwarding packets based on their *destination address field* and/or *protocol type* field.

The filtering process works in the following manner:

- Each bridge module has a *static-address table* which contains a list of user specified MAC addresses plus a filter for each of these MAC addresses which can be one of the following:

  – *always_forward*

  – *never_forward_to_port1*

  – *never_forward_to_port2*

  When a packet is received, the destination address will be compared with the entries in the static-address table, if the packet is not allowed to be forwarded it will be discarded by the bridge module.

  If the packet is allowed to be forwarded, it will be passed to the *protocol-id filter*.

- Each bridge module has a *protocol-id table* which contains a list of protocol-ids. Also, the user can set one of the following modes for the protocol-id table (which applies to all its entries):

  – *disable*

  – *forward*

  – *filter*

  When a packet is to pass through the *address filter*, if the mode setting for the protocol-id table is *disable*, no further filtering is done and the packet is forwarded. But, if the protocol-id table mode is *filter* or *forward*, the packet will go through further filtering as follows:

  The *protocol type* of the packets is compared against the contents of the protocol-id table.

  – If a match is found and the mode is *forward*, then the packet is forwarded.

  – If no match is found and the mode is *forward*, the packet is discarded.

  – If a match is found and the mode is *filter*, the packet is discarded.

  – If a match is not found and the mode is *filter*, the packet is forwarded.

  Before the changes specified by the *set filter* command for the *static-address table* to take effect, the changes must be *saved* and the bridge module must be *reset*. So, you must ensure that you issue *save filter* and *reset device* commands after modifying the entries in the *static-address table*. Pressing the *reset button* has the same effect as issuing the *reset device* command.

Note

Traffic forwarding will be interrupted for a short time when you reset the bridge.

7.8.2.4 Set Spanning Tree Parameters

set spantree command is used to control all of the spanning tree parameters. After changing the spanning tree parameters, they will become active immediately. The parameters you can change are the following:

- Bridge_priority

  Bridge_priority is used in conjunction with the Ethernet address of the bridge to determine which bridge becomes the root bridge in the network. The parameter used to determine the root bridge is the most significant portion of a numeric value which consists of the *bridge_priority* and the *Ethernet address of the bridge*. The default setting for the *bridge_priority* is 128 which can be over-written using the following command:

  ```
  SET SPANTREE BRIDGE_PRIORITY nnn
  ```

- Forward_delay_time

  This parameter specifies the amount of time bridges wait in each state when moving from *listening* to *forwarding* mode. In other words, this is the amount of time a bridge will stay in each of these two states before taking over as the *designated bridge*. The default value for this parameter is 15 seconds which can be changed using the following command:

  ```
  SET SPANTREE FORWARD_DELAY_TIME nn
  ```

  where *nn* can be between 4 and 30. Note that changing this parameter has no effect until this bridge becomes the root bridge. This is because all the bridges in a network use the *forward_delay_time* specified in the root bridge.

- Hello_time

  This parameter specifies how often this bridge sends out *hello* packets when it becomes the root bridge. The default value for this parameter is 2 seconds which can be changed using the following command:

  ```
  SET SPANTREE HELLO_TIME nn
  ```

  where *nn* can be between 2 and 10. Note that changing this parameter has no effect until this bridge becomes the root bridge.

- Listen_time

  This parameter specifies how long this bridge will wait for the root bridge to send out hello packets. If a bridge does not receive a hello packet within the time specified by this parameter, it will assume the root bridge is not active and begin to try and establish itself as the root bridge. The default value for this parameter is 20 seconds which can be changed using the following command:

  ```
  SET SPANTREE LISTEN_TIME nn
  ```

  where *nn* can be between 6 and 40. Note that changing this parameter has no effect until this bridge becomes the root bridge.

  If you decide to change the default values for *forward-delay time*, *hello_time* and *listen_time* you must use the following two formulas:

```
2*(forward_delay_time - 1.0 Sec)  >=  listen_time
```

```
listen_time >= 2* (hello-time + 1.0 Sec)
```

- Spanning tree mode

  This parameter is used to enable/disable the spanning tree protocol in the bridge module. The default for this parameter is *enabled* and can be changed via the following command:

  ```
  SET SPANTREE MODE DISABLE/ENABLE
  ```

- Path_cost_port1

  Use the following command to the change the default (10) *path_cost* for *port1* on the bridge module:

  ```
  SET SPANTREE PATH_COST_PORT1 nnnnn
  ```

  where *nn* can be between 1 and 65,535.

- Path_cost_port2

  Use the following command to change the default (10) *path_cost* for *port2* on the bridge module:

  ```
  SET SPANTREE PATH_COST_PORT2 nnnnn
  ```

  where *nn* can be between 1 and 65,535. Note that changing the path_cost for an active bridge in the network could result in changes in the *blocking/forwarding* state of that bridge. Also, it may cause other bridges, for which this bridge is the *designated* bridge, to change their path to the root bridge.

- Spanning tree hello_address

  Use the following command to change the default spanning tree *hello_address* for the bridge module:

  ```
  SET SPANTREE HELLO_ADDRESS XX-XX-XX-XX-XX-XX
  ```

  This is the *Group MAC Address* that the Bridge Protocol Data Units (BPDU) are transmitted to. All the bridges taking part in the spanning tree protocol must use the same address. The address defined by IEEE to be used as the spanning tree hello_address is 800143000000.

  The only time that this address may be required to be changed is when the bridge module is going to inter-operate within a network where there are some old bridges which do not use the IEEE-specified address for the spanning tree hello_address.

- Disable dip switch setting

  By default, the bridge module will use the onboard dip switch settings to configure the networks for the bridge module when it is re-booted. If you set the networks through a management module or the bridge module, you need to issue the following command to ensure that in the future, the network configuration is read from the memory on the module, rather than using the dip switches:

  ```
  SET BRIDGE DIP_CONFIGURATION DISABLE
  ```

Note

Network selection and other parameters are stored in non-volatile memory on the bridge.

- Select the networks to be bridged

  The networks to be bridged by the bridge module can be selected in the following ways:

  – If you have a terminal attached to the RS-232 port on the bridge module, you can issue the following command to select the networks:

    ```
    SET BRIDGE CHANNEL PORTn m
    ```

    where *n* the port number (1 or 2) on the bridge module and *m* is is the backplane network number (1, 2, 3 or isolated). When you are setting the network for port 1, 3 is not a valid option. Instead you can specify *front* which means that the bridge module will use the AUI port to connect to one of the networks.

  – If you are using a management module, use the following command to select the networks:

    ```
        SET PORT x.y CHANNEL z
    ```

    where *x* is the leftmost slot on the 8250 occupied by the bridge module, *y* is the port number (1 or 2) on the bridge module and *z* is the same as *m* described in the previous step.

    Note: You can do a remote login from the Ethernet management module to the bridge module and then issue the *set bridge channel* command instead of the management module′s *set port channel* command.

  – If you do not have a terminal connected to either the management module or to the bridge module, you can perform channel selection via the onboard dip switches on the bridge module.

  To ensure that the parameters set for the bridge module are used the next time you re-boot the 8250 or the bridge module, you should issue a *save* command to store these parameters in the non-volatile memory of the bridge module.

7.8.3 Management of Bridge Module

The bridge module can be managed *out-of-band* using an ASCII terminal connected to the RS-232 port which is provided on the front panel of the bridge module. This terminal can be local or can communicate over a telecommunication line at speeds up to 9600 bps.

A bridge module can also be managed from an ASCII terminal connected to a second bridge module installed on the same or another 8250. This can be done by issuing a *remote_login* command from the ASCII terminal. Note that you need to provide the name, IP address, or the MAC address of the bridge module in the *remote_login* command and should also provide the correct password.

You can also do a *remote-login* to a bridge module from an ASCII terminal attached to an Ethernet management module.

You can also manage an Ethernet bridge remotely, using an SNMP workstation such as an RS/6000 using AIX NetView Hub Management Program/6000. For detailed information about the management of bridge modules, refer to 14.1.3, “ Ethernet Bridge Module - In-Band Management” on page 324.

7.9 IBM Ethernet Transceivers

While more and more devices are being made available with onboard transceivers, there are still many instances where an external transceiver is required. The following transceivers are available via IBM to complement the IBM 8250 Multiprotocol Intelligent Hub family.

7.9.1 10BASE-T Transceiver

The 10BASE-T transceiver is a one-port transceiver that complies with the 10BASE-T standard. It can be used to connect a DTE or a repeater port to the 10BASE-T modules on the IBM 8250.

The 10BASE-T transceiver provides an RJ-45 connector at the front and an AUI connector at the rear. There are also a number of dip switches and LEDs. The dip switches are used to set options such as *SQE test* and *link integrity*. The LEDs are used to provide status information about the link. For information about the dip switches and the LEDs, refer to the documentation provided with the 10BASE-T transceiver.

7.9.2 Ethernet Fiber Optic Transceiver

The Ethernet fiber optic transceiver is a one-port transceiver that can be used to provide fiber connection for 802.3 and Ethernet devices to the 8250 fiber modules.

This transceiver provides an SMT, FC or ST connector at the front and an AUI connector at the rear.

There is an LED on the front panel which displays status information about this port. For ease of use, a table is printed on the front panel that briefly describes the meaning of the various status displays shown by this LED.

On the rear panel of this transceiver, there are a number of dip switches which allow you to set the following:

- SQE test
- Alternate collision mode
- Full-step signalling

For more information about the Ethernet fiber optic transceiver, refer to the documentation shipped with the transceiver.

7.9.3 Ethernet FOIRL Transceiver

The Ethernet FOIRL transceiver is a one-port transceiver that complies with the FOIRL standard and can be used to provide connection from 802.3 and Ethernet devices to the 8250 FOIRL modules.

This transceiver provides an SMT, FC or ST connector at the front and an AUI connector at the rear.

There are three activity indicator LEDs and one status indicator LED on the front panel which display *transmit*, *receive* and *collision* information as well as status information about the link.

The dip switches on the front panel allow you to set the *SQE test* option.

For more information about the Ethernet FOIRL transceiver, refer to the documentation shipped with the transceiver.

7.10 Fault-Tolerant Transceivers

In situations where availability is critical, it may be desirable to provide a device with two paths to the LAN. One way to meet this requirement is to provide two separate links from the DTE back to the LAN. The connectivity for this requires the use of a transceiver that can sense when a link is defective and switch to the alternate path. IBM provides the following two transceivers with fault-tolerant capabilities:

7.10.1 Fault-Tolerant 10BASE-T Transceiver

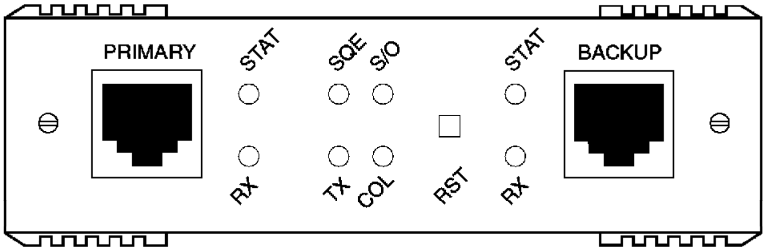


Figure 95. Front View of the Fault-Tolerant 10BASE-T Transceiver

The fault-tolerant 10BASE-T transceiver provides highly-reliable low-cost connections for IEEE 802.3 and Ethernet V2.0 devices.

It can be used to provide fault-tolerant links between the network and a mission-critical Ethernet station, using copper wiring.

It provides two RJ-45 ports (1 primary port and 1 backup port) on the front panel and an AUI interface in the rear panel.

To achieve fault tolerance, the fault-tolerant 10BASE-T transceiver features dual link connections, primary and backup, running from the working area to 10BASE-T ports located on a single hub, or on different hubs but linked in a single Ethernet segment. Any primary link failure between the hub and the fault-tolerant 10BASE-T transceiver causes automatic switch-over to the backup connection that keeps the connection up and running, generally with no noticeable disruption. The fault-tolerant 10Base-T transceiver switches from primary connection to backup whenever it detects one of the following conditions:

- A link integrity error (cable severed or detached) or link integrity disabled by network management
- More than 63 consecutive collisions (looping conditions, short circuit)

For more information about the fault-tolerant 10BASE-T transceiver, refer to the documentation shipped with the transceiver.

7.10.2 Fault-Tolerant Fiber Transceiver

The fault-tolerant fiber transceiver provides highly-reliable low-cost connections for IEEE 802.3 and Ethernet V2.0 devices.

It provides two fiber ports (1 primary port and 1 backup port) on the front panel and an AUI interface in the rear panel. This transceiver can be ordered with SMA, FC or ST type connectors for the fiber.

The fault-tolerant fiber transceiver can be used to provide two connections from a single station to two different ports on an 8250. These ports can be on the same or different modules within the same 8250 (the latter requires the use of advanced management modules). In such a configuration, the primary link will carry all the traffic while the backup link is idle. Any failure in the primary connection will cause an automatic switch-over (in less than 1 millisecond) to the backup link that keeps the connection up and running with no noticeable disruption.

There are five LED indicators on the front panel which provide the user with information about the status of the primary and backup links as well as *data transmission*, *collision* and *switch-over* (from primary to backup).

There are also seven dip switches on the rear panel which will allow you to set the following:

- SQE test
- Normal collision mode
- Transceiver mode
- Full-step signalling
- Optical power mode for primary port
- Optical power mode for backup port

For more information about the LED indicators and the dip switches, refer to the documentation which is shipped with the transceiver.

7.11 Ethernet Management Module

An Ethernet management module can plug into any slot in the IBM 8250 and if configured as the *master management module*, can communicate with all other modules installed in the 8250, via a dedicated control bus, to provide you with the ability to configure the 8250 and its modules according to your requirements. It can also be used to monitor *only* the network to which it is attached.

Two versions of the Ethernet management module are available which are referred to as *basic* and *advanced* Ethernet management modules. These two versions are physically identical. The additional function in the advanced management module is provided through the firmware loaded on the module. The functions provided by these two models are compared in Table 35 on page 186.

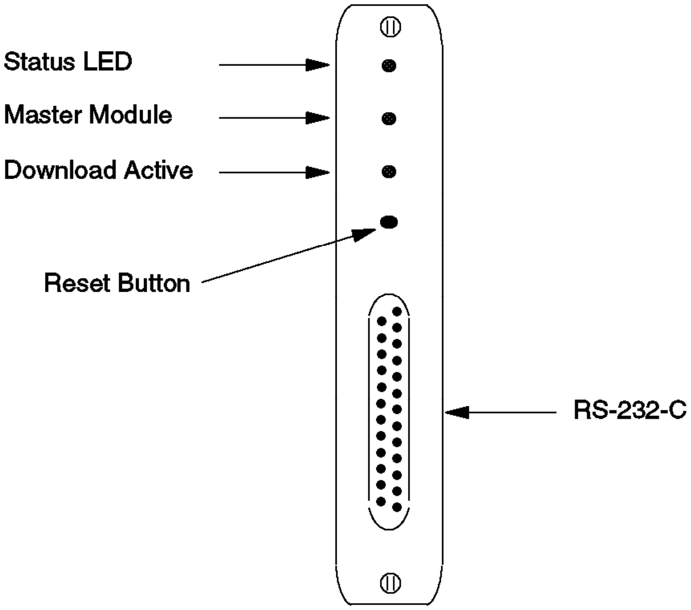


Figure 96. Front view of the Ethernet Management module

The Ethernet Management Module has three LEDs, a *reset button* and an RS-232 port on its front panel as shown in Figure 96. The following table describes what these LEDs mean.

Table 33. Ethernet Management Module LED Descriptions

LED Name	Color	State	Description
Status	Green	OFF	Power off.
		ON	Power on.
		Blinking	Error.
Master Module	Green	OFF	EMM is slave.
		ON	EMM is master.
		Blinking	Mastership election in progress.
Download Active	Yellow	OFF	Not downloading.
		ON	Downloading new software.

The **Reset** Button resets the EMM. It is recessed to prevent an accidental reset. This button can be pressed with a pen tip or small screwdriver. When you press the EMM′s reset button, self-test diagnostic routines execute, but network traffic is not affected. You should press this button *only* when you suspect problems with the EMM.

If the EMM is the master management module, pressing this button will result in the the EMM coming up with the last saved configurations. Therefore, you should save configuration values *before* resetting the module.

The RS-232 port allows an ASCII terminal to be attached to this module for management purposes.

7.11.1 Basic Ethernet Management Module Features

The basic Ethernet management module provides the following capabilities:

- In-band and out-of-band management

  In-band management is defined as management using the SNMP protocol.

  Out-of-band management is defined as management via the RS-232 interface on the 8250 EMM or via a pseudo-console, for example, remote-login from another Ethernet management module.

- Dynamic network control to module/port/bank

  Through the EMM you can dynamically control modules, ports or banks, subject to the functionality of the actual media modules. For instance, if you have a port-switchable fiber module, you could, through an EMM, dynamically switch any of the ports on that module to any one of the three possible Ethernet networks on the backplane.

- Remote configuration of modules/concentrators

  Through the use of the *set* command you can set various attributes of the module/port according to your requirements. For example, you can:

  – Assign a module/port to a specific network

  – Set mastership priority for the EMM

  – Override module-specific dip switch settings

- Automatic detection of faults/failures

  Through the use of the *control bus* all media modules in an 8250 will send error information, specific to their module, to an EMM.

- Continuous monitoring/reporting of key network statistics

  When an EMM is attached to a specific Ethernet network on the backplane, it can gather network statistics about that Ethernet network.

7.11.2 Getting Started with an EMM

Once the EMM has been installed in the 8250, the following should be done:

- Configure the terminal attached to the RS-232 port.
- Configure the EMM.
- Configure the EMM SNMP values (for in-band management only).

7.11.3 Configuring the Terminal

You must initially configure your terminal to the same parameter settings as the EMM so that the terminal and EMM can communicate. You must match the EMM factory defaults as shown in Table 34.

Table 34. EMM Terminal Parameter Options and Defaults

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

Note

Note that the default settings for the TRMM and EMM are different. The EMM requires a setting of *2* for *stop_bits*, while the TRMM requires a setting of *1*.

7.11.4 Configuring the EMM

Once the terminal settings are done, you can configure the EMM and all other 8250 modules. It is recommended that when using the EMM for the first time, you:

- Establish passwords.
- Set the internal clock.
- Configure other EMM parameters.
- Set EMM SNMP values.
- Set EMM terminal for modem connection (if required).

7.11.4.1 Establishing Passwords

The EMM has two levels of password control:

- Administrator

  This provides access to *all* EMM commands, enabling you to display and modify the configuration of the 8250 and its modules.

- User

  This provides *limited* access to EMM commands, enabling you to only display the configuration information about the 8250 and its modules.

To change the password you can enter the following command:

```
SET DEVICE PASSWORD {ADMINISTRATOR or USER}
```

You will then be prompted to enter the new *password*. You must enter the password within 10 seconds of receiving the password prompt, or the terminal will *timeout*. If this happens, just press *Enter* to receive the password prompt again. Both levels of passwords can be up to *15* characters.

The new passwords you set are in effect immediately, but you must use the *save device* or *save all* command to save the new passwords before you re-boot the EMM or the 8250.

Default Administrator password is *nulls* (ENTER).

7.11.4.2 Setting the Internal Clock

The EMM has an internal clock used for time-stamping of SNMP traps. It is set via the *set clock* command. The clock is battery powered with an expected life of 10 years.

Setting the clock is recommended but not mandatory.

7.11.4.3 Configuring Other EMM Parameters

The EMM is set to certain factory defaults. As an administrator you can *set* the following:

- EMM name

  To make communication with your remote EMMs easier, it is recommended that you assign a unique *name* to each EMM. This name can be used to reference a specific EMM instead of the IP address or Ethernet MAC address. In this manner you can log into a remote EMM or ping an EMM using its name rather than its IP address. You can use the following command to set the *name* for EMM:

  ```
  SET DEVICE NAME {name}
  ```

  name can be up to 31 characters long.

- Contact name and location

  You should enter the name of an appropriate service contact and the location of the 8250 using the following commands:

  ```
  SET DEVICE CONTACT

  SET DEVICE LOCATION
  ```

  These commands will prompt you to enter one line of text for *contact* and *location*.

- 8250 re-boot values

  When the EMM is reset (or re-booted) using the factory defaults, the module performs a full diagnostic check and then sets the configuration of all the modules to the settings stored in its memory. You have the option to disable those diagnostics via the following command:

  ```
  SET DEVICE DIAGNOSTICS {enable or disable}
  ```

  This will result in the EMM booting faster.

  You also have the option to have the modules start up according to their dip switch settings (hardware settings) instead of the settings stored in the EMM memory. Although this is not recommended, you can do this by issuing the following command:

  ```
  SET DEVICE DIP_CONFIGURATION {enable or disable}
  ```

- Platform type

  You should specify whether this EMM is installed in an IBM 8250 Model 017 or Model 006, using the following command:

  ```
  SET CONCENTRATOR PLATFORM {hub type}
  ```

  The reason that you should do this is that the 8250 Hub Management Program/6000 will communicate with the XMM in the 8250, and based on this parameter will build the graphical representation of the 8250.

- Command prompt

  It′s a good idea to customize the command prompt for each EMM. This will remind you which EMM you are connected to in the case where you are logged into a remote EMM. The command prompt can be set using the following command:

  ```
  SET TERMINAL PROMPT {prompt}
  ```

- Terminal timeout value

You should set the *terminal timeout* value to specify the amount of time your terminal will remain logged in without any keyboard activity. Once the timeout value has been set, the terminal automatically logs you off the system if there is no keyboard activity for that period of time. This is a good security feature. The following command can be used to set the terminal timeout value:

```
SET TERMINAL TIMEOUT
```

The default timeout value is *0*. This means that you will never be logged-off automatically.

- Mastership priority

  When there are multiple EMMs (or XMMs) within an 8250, and you have not altered the *mastership priority* of any of them, they all have a default priority of *10*. The first EMM to activate in an 8250 will become the *master* and all others will be *slaves*. To ensure that the preferred XMM becomes the master, change the mastership priority of all the XMMs so that the intended master has the highest priority. The format of the command to change the mastership priority is as follows:

  ```
  SET MODULE {slot} MASTERSHIP_PRIORITY nn
  ```

7.11.5 Configuring SNMP Values

If you plan to manage this 8250 through an SNMP management station, you must *set* the following:

1. IP address

   To run SNMP, every device on the network must have a unique IP address. You can use the following command to set the IP address for EMM:

   ```
   SET DEVICE IP_ADDRESS {ip address} {network}
   ```

   You can set a separate IP address for EMM on each of the backplane networks to which it may attach.

2. Community table

   The community table defines the SNMP stations which can access the EMM MIB. You should also define the type of access authorized for each user. Additionally, you can specify the SNMP stations that will receive *traps* from the EMM. The format of the command used is as follows:

   ```
   SET COMMUNITY {community name} {ip address} {access}
   ```

   Where *access* can be:

   - Read-only
   - Read-write
   - Trap
   - Read-trap
   - All

   Note the SNMP manager must supply the specified *community name* in all the SNMP packets that it sends to the EMM, in order to access the EMM MIB according to the access authority defined for that SNMP manager.

3. Default gateway

   The default gateway is the IP address of the *gateway* that will be used to receive and forward packets to the stations whose addresses are unknown in the local network. The default gateway is useful when EMM is sending *traps* to an SNMP manager that is on a different network and is accessible via the defined gateway. You can use the following command to define the default-gateway:

```
SET DEVICE DEFAULT_GATEWAY {ip address} {network}
```

Note that you can define separate default_gateways for each backplane network to which the EMM can attach.

4. Subnetwork mask

   You can use the following command to specify the *subnetwork mask* to be used by the EMM when attached to a specific network on the backplane:

   ```
   SET DEVICE SUBNET_MASK {mask} {network}
   ```

   More information about subnetwork mask can be found in 4.3, "IP Subnets" on page 76.

5. Alerts

   The *set alert* command is used to enable or disable the sending of a *trap* to an SNMP manager station. The format of the *set alert* command is as follows:

   ```
   SET ALERT {alert type} {enable or disable}
   ```

   Alert types are:

   - *Authentication*

     This type of trap is sent when someone tries to access the EMM and their IP address or community name is not valid for the attempted read or write operation.

   - *Change*

     This type of trap is sent when a configuration change is made to this 8250.

   - *Hello*

     This type of trap is sent when an existing EMM is reset in the 8250. This trap is sent once every minute until a valid SNMP acknowledgment is received from the SNMP manager station, or for up to 4 hours and 15 minutes, at which time the sending of the trap will be stopped.

   Note that the default setting is *disabled* for all three options.

7.11.6 Set EMM Terminal for Modem Connection

If you are going to access the EMM via a Modem, the Terminal options will need to be set to match the modem′s capabilities. The *set terminal* command is used to set the options required.

7.11.7 Other EMM Commands

The EMM module has a full set of commands available to allow you to *show* and *set*, the configuration parameters of the EMM and the other modules installed in the 8250. Also, you can collect statistical information about the network to which the EMM is attached. For information about these functions, refer to Chapter 14, "Ethernet Management Functions" on page 303.

7.11.8 Advanced Ethernet Management Module

The advanced version of the EMM represents significant enhancements in several key areas: fault tolerance, port security, SNMP network monitoring and in-band software download.

- Fault tolerance

  The advanced EMM allows any two ports to be designated as the primary port and backup port. These ports can exist on any modules within the 8250 regardless of media type. For example, the primary port could be a fiber port on module 3, port 4, while the backup port could be a twisted-pair port on module 8, port 2. In addition, the backup port does not have to be on the same network with the primary port, but it must be running the same protocol.

- Port security

  The advanced EMM can identify any port in the 8250 and protect it against unauthorized access by restricting access on that port to specific Ethernet MAC address(es). If the Ethernet address should change at that port, the EMM will issue a *trap* to all management stations identified in the community table, and will shut down the port if configured to do so. The advanced EMM has the ability to assign 1024 Ethernet addresses for security.

- Network-wide error monitoring

  The advanced EMM can receive any SNMP trap from any SNMP-compliant vendor′s network device. If the trap is from an 8250 device, the EMM will provide and interpret alarm messages to the operator. It will also forward the trap to the SNMP manager station if available. If the trap is from a non-8250 device, the EMM will pass the information directly to the operator without interpretation. Also, these traps will not be forwarded to the SNMP manager station.

- Supports in-band download

  The advanced EMM enables the administrator to load new software into all EMMs over the network using FTP file transfer between the workstation (or any FTP server) and the EMM.

7.11.9 Comparison of Basic and Advanced Management Module Function

Table 35 provides a summary of the functions provided by the basic and advanced EMM.

Table 35 (Page 1 of 2). Advanced vs Basic EMM Function

Function	Basic EMM	Advanced EMM
Protocols Supported	Ethernet, TR, FDDI	Ethernet, TR, FDDI
Number Ethernet Networks	3	3
Improved Network Protection	Yes	Yes
Integrates into SNMP Systems	Yes	Yes
Configure and Monitor Status	Yes	Yes
Network Map	Yes	Yes

Table 35 (Page 2 of 2). Advanced vs Basic EMM Function

In-band download from Servers	No	Yes
Increased Port Security	No	Yes
Receives SNMP Traps from ANY Device	No	Yes
Alarm if Port Address Changes	No	Yes
Disable Port when MAC Changes	No	Yes
Cross Module Redundancy	No	Yes
Cross Module Redundancy Across Networks	No	Yes

Chapter 8. Ethernet Terminal Server Module

This chapter contains a brief description and configuration information about the Ethernet terminal server module.

Because of the range of functions and variety of possible configurations offered by the terminal server module it is not the intention of this chapter to provide every detail about all the features of the Ethernet terminal server module. Therefore, the reader is referred to the *Ethernet Terminal Server Reference Guide* for additional information.

8.1 Ethernet Terminal Server Module

The Ethernet terminal server module provides 16 asynchronous ports which are used to attach terminals, printers, modems and other serial devices to the terminal server. The terminal server, will in turn be connected to an Ethernet network over the 8250 backplane, allowing it to provide its asynchronous ports with access to the services available on the Ethernet network. These services can be accessed using LAT and/or TCP/IP protocol. Also, through a function called *Network Protocol Translation (NPT)*, the terminal server can be configured to allow TCP/IP devices to access LAT services and LAT devices to access TCP/IP services.

Figure 97 provides a summary of the functions provided by the 8250 Ethernet terminal server module.

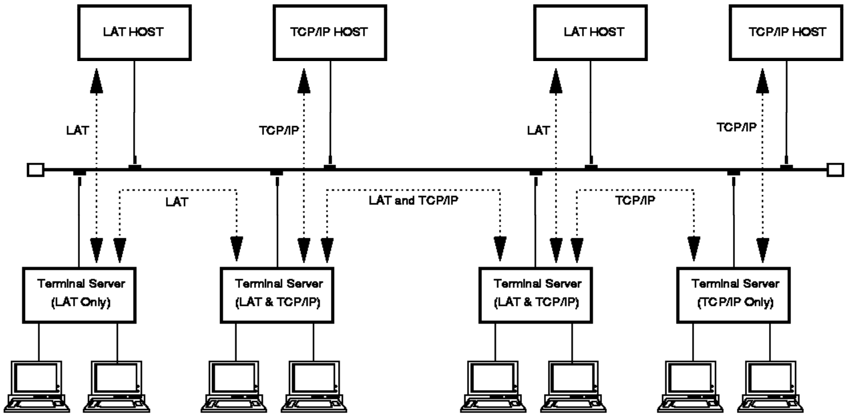

LAT HOST
TCP/IP HOST
LAT HOST
TCP/IP HOST
LAT
TCP/IP
LAT
TCP/IP
LAT
LAT and TCP/IP
TCP/IP
Terminal Server (LAT Only)
Terminal Server (LAT & TCP/IP)
Terminal Server (LAT & TCP/IP)
Terminal Server (TCP/IP Only)

Figure 97. Ethernet Terminal Server

The following are some of the reasons for using the Ethernet terminal server module:

- Once a terminal is connected to a host via the terminal server, the host will be relieved from the task of maintaining the connection to the terminals. Also, the terminal server will perform all the functions necessary to exchange data with the terminal. This will reduce the processing overhead on the host, allowing it to run the applications more efficiently.

- Using terminal servers will allow a single connection from a TCP/IP or LAT hosts to the Ethernet network to provide the necessary connection required to enable many asynchronous terminals to access the services offered by that host.
- Terminal servers will allow the terminals attached to them to access many TCP/IP and LAT host via a single connection. This allows you to offer multiple services to a user without having to provide multiple connections. Also, in case of the failure of a service, backup can easily be provided using one of the operational hosts on the network.
- TCP/IP and LAT hosts which do not have an Ethernet connection, can be connected to the LAN via the asynchronous ports on the terminal server. This would allow such hosts to communicate with the other TCP/IP and LAT hosts on the network as well as making their services available to the terminals connected to the network via terminal servers.

The terminal server supports the following protocols:

- LAT
- TCP/IP
- SNMP
- PPP
- SLIP

Note that the terminal server uses the Ethernet V2 frame format to communicate over the network and is not capable of communicating with devices that use the IEEE 802.3 frame format.

8.2 Terminal Server Module Installation

Figure 98 on page 191 shows the front view of the terminal server module.

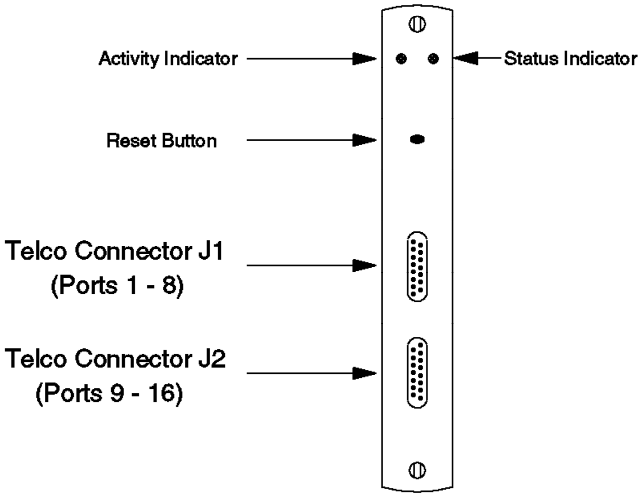


Figure 98. Front View of the Terminal Server Module

Each *telco connector* provides connections for up to 8 asynchronous devices by using a harmonica or a patch panel.

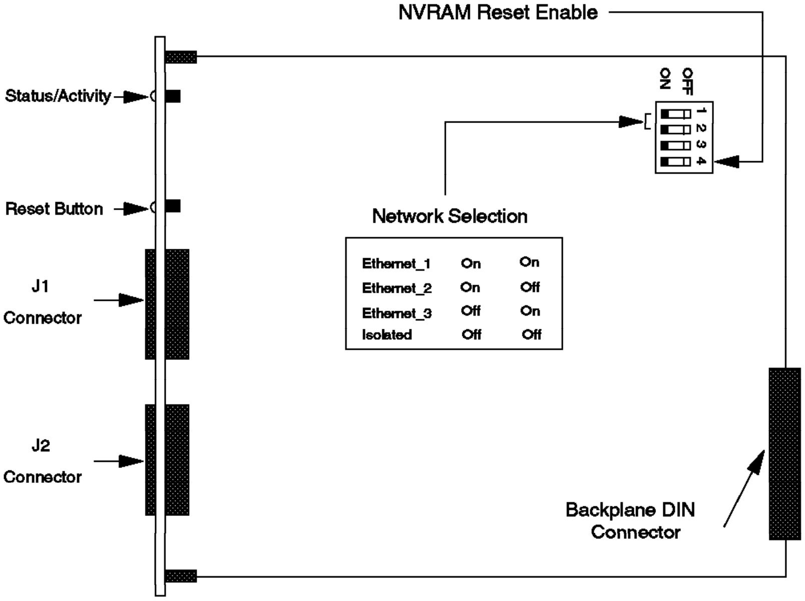
When pressed, the *Reset button* causes the terminal server to reboot.

The following table describes what the *activity* and *status* LEDs mean.

Table 36. Terminal Server LED Description

LED name	Color	State	Description
Activity	Yellow	OFF	No packets are being transmitted.
		ON	Packets are being transmitted to the network.
Status	Green	OFF	Power off.
		ON	Power on.

Figure 99 on page 192 shows the terminal server dip switches, their meanings and their factory settings.



Ethernet_1	On	On
Ethernet_2	On	Off
Ethernet_3	Off	On
Isolated	Off	Off

Figure 99. Side View of the Terminal Server Module

8.3 Configuring Terminal Server Module

To configure the terminal server module, you must do the following:

- Assign the module to a network

  A terminal server module can be assigned to any Ethernet network or set to isolated. This can be done via dip switch settings or the following management module command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

  If there is a management module installed on the 8250, the dip switch settings for network selection will be ignored.

- Set port mode for each port

  Using the management module you can set one of the following *modes* for each port:

  - Local: enables only the *incoming* connections to the terminal server from serial devices.
  - Remote: enables only the *out-going* connections from the terminal server.
  - Enable: enables both *incoming* and *out-going* connections to/from the terminal server.
  - Disable: disables the port.

  The format of the command to set the mode for the terminal server ports is as follows:

  ```
  SET PORT {slot.port} MODE {enable/disable/local/remote}
  ```

- Set NVRAM (Non-Volatile RAM) reset enable

There is a dip switch onboard the terminal server module called *NVRAM Reset Enable*. If this switch is set *ON*, it will cause the module to restore its permanent database (in the non-volatile RAM) to its factory settings every time the module is rebooted. It is recommended that this switch be set to the *OFF* position, except when an intentional reset of the module′s non-volatile RAM is required.

Note that this switch cannot be set via a management module command. However, there is a *reset* command which will allow you to reset the module′s permanent database to its factory setting.

8.4 Customization of the Terminal Server

In addition to the configuration of the terminal server as described above, you must customize the terminal server to address the requirements of your installation. The initial customization of the terminal server can be done via a terminal attached to the terminal server. After the initial customization, if you have defined Telnet service within the terminal server, you can do the subsequent customization via a terminal logged in to the terminal server using Telnet.

The customization process defines the information concerning:

- Port definitions
- Terminal server characteristics
- Service definitions

The customization information is stored within the terminal server in two different places. These are referred to as:

- Run-time (temporary) configuration database, and
- Permanent database

The information in the *run-time* database is valid for the duration of the current operation of the terminal server. This information will be lost once the terminal server is reinitialized.

The *permanent* database contains the information that will be used during the initialization of the terminal server unless the *NVRAM reset enable* switch is set *ON*.

The terminal server commands available to make changes to one or both of these databases are:

- **Set**

  Changes the run-time database settings. The effects of this command are immediate and since they affect the run-time database only, the changes will be lost once the terminal server is reinitialized.

- **Define**

  Changes the permanent database settings. This command does not affect the current operation of the terminal server. Its effects will be seen after the terminal server is reinitialized.

- **Change**

Changes **both** the run-time and permanent databases. The effects of this command are immediate.

- **Clear**

  Removes entries from the run-time database.

- **Purge**

  Removes entries from the permanent database.

- **Show**

  Views run-time database entries.

- **List**

  Views permanent database entries.

- **Monitor**

  Allows viewing the run-time database entries with periodic updates.

Detailed information about terminal server customization and its commands are provided in *Terminal Server Reference Guide (SA33-0206)*. The following is an overview of the steps necessary to customize the terminal server.

8.4.1 Connecting a Terminal to the Terminal Server

Once you have configured and installed a terminal server as described in 8.3, “Configuring Terminal Server Module” on page 192, you should connect a terminal to one of its ports to begin the customization tasks.

The terminal must be an ASCII terminal with the following characteristics:

```
Baud         9600
Data bits    8
Parity       None
Stop bits    1
```

Throughout our residency, we used a PS/2 running DOS operating system and the IBM FTTERM V 2.1 to emulate a DEC** VT100**.

8.4.2 Customization of Terminal Server Ports

After connecting the terminal and pressing the *Enter* key, the following will be displayed:

```
Chipcom OETS V6.303

Please type HELP if you need assistance

Enter username>
```

The *username* is used by the terminal server to identify the users on each port. You can enter up to 15 alphanumeric characters as the username. You are advised to use your name for this purpose.

After entering the username, the terminal server′s *prompt* will be displayed. The following is the default prompt:

```
LOCAL>
```

To perform all the customization tasks, you require *privileged* access to the terminal server. You can gain privileged access by entering the following command:

```
SET PRIVILEGED
```

You will then be asked to enter a *password*. The default password is *SYSTEM*.

At this stage, you are advised to change the password for privileged access by entering the following command:

```
CHANGE SERVER PRIVILEGED PASSWORD nnnnnn
```

where *nnnnnn* is up to 6 characters. Note that this password is a parameter that is defined for the *server* and is not port specific.

Once you are connected to a port, you use the following command to view the characteristics of the terminal server ports:

```
SHOW PORT 1 CHARACTERISTICS
```

The resulting display will be as follows:

```
 Port 1:  shabani

 Character Size:           8          Input Speed:        9600
 Flow Control:           XON          Output Speed:       9600
 Parity:                None          Modem Control:  Disabled
 Stop Bits:                1          Profile:
 Access:               Local          Local Switch:       None
 Backwards Switch:      None          Name:             PORT_1
 Break:                Local          Session Limit:         4
 Forwards Switch:       None          Type:               Soft
 XON Char:                [Q          XOFF Char:            [S
 Preferred Service: None
 Virtual Login:     None

 Authorized Groups:   0
 (Current)  Groups:   0

 Enabled Characteristics:

 Autobaud,  Autoprompt,  Broadcast,  Input Flow Control,  I/O Flush,
 Linemode,  Loss Notification,  Logout Message,  Message Codes,
 Output Flow Control,  Verification

 Local>
```

These characteristics can be changed (temporarily or permanently) using the *set port*, *change port* and/or *define port* commands.. These commands can be used to change the characteristics of a single port or all ports.

It is not our intention to cover all the port parameters that can be changed using these commands. However, to ensure that the reader is familiar with some of the options, the following examples are provided:

```
CHANGE PORT 1 CHARACTER SIZE 7
```

This command allows you to specify the number of bits used within the characters exchanged between the ASCII terminal and the terminal server. Default is 8 bits.

```
CHANGE PORT 1 PARITY odd
```

This command allows you to specify the type of *parity bit* used within the characters exchanged between the ASCII terminal and the terminal server. Default is *none*. The other options are *even*, *mark* and *space*.

```
CHANGE PORT 1 STOP BITS 2
```

This command allows you to specify the number of *stop bits* used within the characters exchanged between the ASCII terminal and the terminal server. Default is *one*.

```
CHANGE PORT 1 TYPE ansi
```

When a terminal is *locally* connected to the terminal server, all the control functions (such as backspace) are performed by the terminal server. Therefore, when using local terminals you should use the above command to ensure that the terminal server properly executes the control operations performed at the terminal. Default for this option is *softcopy* which designates a non-ANSI device such as VT-52**. The other option is *hardcopy* which is used to support printers.

```
CHANGE PORT 1 ACCESS local
```

This command allows you to specify how the users are connected to the ports on the terminal server. The *local* option means that the *local* or *modem* attached devices are allowed to use this port to access services available on the network.

The other options are *remote*, *dynamic* and *none*.

The *remote* option is for dial-out devices and printers.

The *dynamic* option allows you to use local and remote access. *None* means that the port is disabled.

```
CHANGE PORT 1 PROMPT input:>
```

This command allows you to change the default *prompt* to a character string of up to 10 alphanumeric characters.

```
CHANGE PORT 1 PASSWORD enabled
```

Using this command will result in the user of the port being prompted (via # character and a *beep* sound) for a password when the terminal is first connected to that port. The user must enter the correct password before he can enter any other command. The password must be the character string which is specified for the server by the following command:

```
CHANGE SERVER LOGIN PASSWORD nnnnnn
```

where *nnnnnn* can be up to six characters. Default password is *ACCESS*.

```
CHANGE PORT 1 SESSION LIMIT n
```

This command specifies the *maximum number of concurrent sessions* that a single local terminal can maintain. The value of *n* can be from 0 to 10. You could also specify *none* which will result in 10 sessions for that port. The default is 4.

Note that the total number of concurrent active sessions on the server cannot exceed the the *session limit* specified for the server by the following command:

```
DEFINE SERVER SESSION LIMIT n
```

where *n* can be a value between 16 and 512. Default is 320.

```
CHANGE PORT 1 USERNAME shabani
```

This command allows you to associate up to 15 alphanumeric characters with a port that will be used by the server to identify the user logging into that port. If you issue this command for a port, and you have disabled the *entry* option (for information on the *entry* option, refer to 8.4.3, “Customizing Server Definitions”) for the terminal server, the user will not be prompted to enter *username* when a terminal is connected to that port. Otherwise, every time a user connects to a port, the server will prompt the user to enter *username*.

```
CHANGE PORT 1 SECURITY enabled
```

This command is used to limit the server commands that can be entered by the user connected to a port. This command may be used if you wish to prevent the users connected to specific ports from issuing commands (such as *show port*) that obtain information about other ports.

```
CHANGE PORT 1 NAME fred
```

This command can be used to assign a *name* to a port which can be used, instead of the *port number*, when accessing this port.

```
CHANGE PORT 1 INACTIVITY LOGOUT enabled
```

This command will result in the server logging out this port if the port is *inactive* for a period of time defined as *inactivity timer* for the server. An inactive port is a port which has no active session and has not generated any I/O during the *inactivity timer* period.

For information on how to define the *inactivity timer* for server, refer to 8.4.3, “Customizing Server Definitions.”

Note that in all of the above examples, we have used the *change* command. However, as discussed earlier, you may use *set* or *change* commands depending on your requirements.

8.4.3 Customizing Server Definitions

Once connected to the terminal server, you can use the following command to display the current *characteristics* of the terminal server:

```
SHOW SERVER CHARACTERISTICS
```

The resulting display is as follows:

```
Chipcom OETS    Version: V6.303                  Uptime:   0  0:07:54

Address:  00-00-B5-0C-08-5E    Name:  LAT_0000B50C085E    Number:     0

Identification:

Absolute Timer:          30          Multicast Timer:          30
Bootserver:            None          Node Limit:              256
Break Length:            27          Password Limit:            3
Circuit Timer:           80          Path:                   None
Console Port:             1          Primary Boot:            ROM
Ethernet:          Thinwire          Queue Limit:              24
Inactivity Timer:        30          Retransmit Limit:         30
Keepalive Timer:         20          Secondary Boot:         None
```

```
Maximum Circuits:         64          Session Limit:          320
Maximum Services:        256          Software:          DSSRV001
Maximum Sessions:         64          XOFF Limit:              16
                                      XON Limit:              496
Service Groups:   0

Enabled Characteristics:
Announcements,  Autoboot,  Broadcast,  Dump,  Entry,  Lock,  Panel

Local>
```

To change the characteristics of the terminal server, you can use *change server*, *set server* or *define server* commands. The following are examples of some of the terminal server characteristics that can be changed:

```
CHANGE SERVER CONSOLE port 5
```

This command allows you to define the terminal server port which will receive all the messages issued by the terminal server. Port 1 is default.

```
CHANGE SERVER ENTRY disabled
```

When a *username* has been defined for a port as explained in 8.4.2, “Customization of Terminal Server Ports” on page 194, and you have issued the above command, the user will not be prompted to enter *username* when he connects to the terminal server.

Enabling this function will result in the user being prompted for the *username* regardless of the port definition.

```
CHANGE SERVER INACTICITY TIMER nnn
```

This command specifies the amount of time that the server will wait before logging out the *inactive* ports. *nnn* is in *minutes* and can range from 0 to 120. Default is 30 minutes.

Note that inactive ports are the ports that have no active session and have not generated any I/O during the *inactivity timer* period.

This timer affects only the ports for which the *port inactivity logout* has been enabled.

```
CHANGE SERVER LOCK enabled
```

This feature allows individual ports to prevent unauthorized access to their terminal, when it is left unattended, through the use of the *lock* command.

Once you have entered the *LOCK* command, the following will be displayed:

```
Lock Password>
```

After entering the password, you will be asked to re-enter the password via the following prompt:

```
Verification>
```

Once the password has been re-entered correctly, the terminal will be locked and the following will be displayed:

```
Local -019- Port nn locked

Unlock Password>
```

where *nn* is the port to which your terminal is connected.

```
CHANGE SERVER PASSWORD LIMIT 5
```

This command defines the maximum number of attempts within which the user of a port should enter the correct password. When the password limit is reached, the user will be logged out and must wait *one* minute before being allowed to try again.

This limit applies to both *port password* and the *privileged password*.

```
CHANGE SERVER SNMP enabled
```

This enables SNMP managers to access the contents of the *run-time* and *permanent* databases. The type of access allowed is specified using the following command:

```
CHANGE SERVER SNMP COMMUNITY readwrite itsc
```

where *readwrite* is the type of allowed access and ITSC is the *community name*. The other permitted options for the access are *read* and *write*.

8.4.4 Customizing Service Definitions

In addition to allowing its attached devices to log in to the terminal server and access TCP/IP and LAT services offered on the network, the terminal server will allow asynchronous devices which are attached and logged on the the hosts attached to the network, to access the services which are offered by the terminal server.

Terminal server provides you with the ability to create local *LAT* and *TCP/IP* services.

Local services can be:

1. Hardware devices, such as printers, attached to the terminal server.
2. Applications which reside in the hosts attached to the terminal server.

Local services can be created using *change service*, *set service* or *define service* commands. The following are some examples of creating local services:

```
CHANGE SERVICE itsclat Port 3 LAT enable
```

This command allows you to create a local *LAT* service called *itsclat* which is offered on port 3 of the terminal server. In this example, the service could be a printer which is attached to port 3 of the terminal server and is accessible to the LAT users.

```
CHANGE SERVICE itsctcp Port 5 TELNET enable TCP PORT 2048
```

This command allows you to create a local *Telnet* service called *itsctcp* which is offered on port 5 of the terminal server. Note that this service is associated with *TCP port 2048*. This, for example, allows you to Telnet to the terminal server from an AIX machine using the following command:

```
telnet 9.67.46.150 2048
```

Where *9.67.46.150* is the IP address of the terminal server. In fact, to be able to provide Telnet services via the terminal server, you must always assign an IP address to the terminal server using the following command:

```
CHANGE SERVER IP ADDRESS 9.67.46.150
```

Note that you must reinitialize the terminal server with the new Telnet service, by issuing the terminal server's *CRASH* command, immediately after defining the IP address.

To simplify the task of terminal server users connecting to Telnet hosts, you may assign a *name* to those hosts using the following command:

```
CHANGE DOMAIN host1 IP ADDRESS 9.67.46.150
```

Alternatively, you may provide the terminal server with access to one or more *name servers* using the following command:

```
CHANGE NAMESERVER  9.67.46.160
```

You can also define one or more *gateways* to the terminal server using the following command:

```
CHANGE ROUTE 3 GATEWAY 9.67.46.166
```

8.5 Using the Server

When you first connect to the terminal server, you are in *local* mode and you see the server's local *prompt*.

After you connect to a service, you are in *session* mode and your terminal will act as though it is directly attached to the host or device providing the service.

You may run several sessions at once and *hot-key* between them. These sessions could be to multiple hosts, or to multiple services on one host. Always, the session you are working on is your *current session*.

8.5.1 Connecting to Services

To display services available through the terminal server you must enter the following command at the prompt:

```
SHOW SERVICES
```

The resulting display is similar to the following:

```
Local> show services


Service Name         Status        Identification

ITSCLAT              Available
ITSCLAT1             Available
ITSCTCP              Available

Local>
```

Detailed information about an individual service can be obtained by using the following command:

```
SHOW SERVICE itsclat CHAR
```

The resulting display is similar to the following:

```
Local> show service itsclat char

Service: ITSCLAT
Identification:
Ports:   1- 32
Rating: 0
Virtual Login: None
Enabled Characteristics:
Connections,  Lat,  Queueing

Local>
```

.To connect to a service enter the following command at the prompt:

1. For LAT service

   ```
   CONNECT LAT {service name}
   ```

2. For Telnet host

   ```
   CONNECT TELNET {host ip address} or {host name}
   ```

The login message for the service will appear requesting:

- User ID
- Password

The following is the output displayed when a login attempt was made to a TRMM using Telnet:

```
Local> connect telnet 9.67.46.138
Local -010- Session 1 to 9.67.46.138 established


8250

Token Ring Management Module (v2.00-B)
Copyright (c) 1992 Chipcom Corporation
Password:
```

Once you are in session, you can return to local mode by pressing the *Break* key. However, some modems will disconnect when they see this key. If you are using such a modem, you will need to use a local switch key in place of the Break key. This can be done using the following command:

```
CHANGE PORT n LOCAL SWITCH {keyboard character}
```

Once the local mode prompt returns, your session is no longer active. However, it is still the *current* session, and can be reactivated with the *RESUME* command.

When you are in the local mode, you can log in to another session. The terminal server supports up to 10 concurrent sessions per port (depending on the session limit specified for that port).

You can get information about all your current sessions using the following command:

```
SHOW SESSIONS
```

The resulting display will be similar to the following:

```
Local> show sessions


Port   1:  shabani          Local Mode   Current Session 2
 - Session  1: Connected     Telnet       9.67.46.138
 - Session  2: Connected     Telnet       RS6000

Local>
```

Note that in the above example, session 2 was established using a *name* rather than an *IP address* in the *CONNECT* command.

When you have multiple sessions, you can return to any one of them by using the *RESUME SESSION* command and specifying a *session number*:

```
RESUME SESSION 1
```

Another way to change between sessions is to use the *FORWARD* and *BACKWARD* commands from the local prompt. *FORWARD* moves you to the next higher-numbered session, making it the current session. *BACKWARD* moves you to the next lower-numbered session, making it the current session.

8.5.2 Disconnecting from a Service

You can disconnect from sessions in two ways:

1. Disconnecting from session mode

   In this case, you must use a service specific *logout* command to terminate your current session.

2. Disconnecting from local mode

   While in *local* mode you can use the following commands to terminate from your *current* session:

   ```
   DISCONNECT
   ```

   To terminate a session other than the current session, you should specify the *session number*, with the *DISCONNECT* command:

   ```
   DISCONNECT SESSION {number of session}
   ```

   You can terminate all the existing sessions for your port using the *all* option of the *DISCONNECT* command:

   ```
   DISCONNECT ALL
   ```

8.6 Terminal Server SLIP Interface

The terminal server module provides support for both *static* and *dynamic* SLIP interfaces.

Static interface requires the server port to be dedicated to the SLIP interface permanently. Dynamic interface allows you to use that server port for SLIP whenever required. This means that when SLIP is not active on that port, the port can be used for other types of connections.

An example of the static SLIP interface is when two terminal servers, each attached to their own Ethernet, are connected to each other using a communication line and a pair of modems. This configuration will allow the stations on the two Ethernet networks to communicate with each other using the link between the two terminal servers.

An example of using dynamic SLIP, is when you have a PS/2 running DOS and the IBM TCP/IP program which during the working hours uses its connection to the Ethernet network to communicate with the other devices attached to the network. After working hours, this PS/2 can dial-in over a communication line and use SLIP to communicate with the network-attached workstations. In this case, the terminal server becomes an IP gateway for the PS/2 running TCP/IP.

To use dynamic SLIP, we configured a PS/2 running DOS to have both IBM FTTERM V2.1 and IBM TCP/IP installed. We first connected the PS/2 via its serial port to one of the terminal server ports. After accessing the server and getting the *privileged* access, we entered the following command:

```
CHANGE ARP 9.67.46.140 Ethernet 00-00-B5-0C-08-5E PROXY enabled
```

Where 9.67.46.140 is the IP address of the PS/2 and 00-00-B5-0C-08-5E is the Ethernet address of the terminal server (Ethernet address of terminal server can be obtained using the SHOW SERVER command).

We then issued the following command to start the SLIP connection:

```
CONNECT SLIP 9.67.46.140
```

When the connection was established, the following message was displayed:

```
Session Established
```

At this stage we used the ALT and PF9 keys to exit from FTTERM. When in DOS, we started TCP/IP for DOS using the *tcpstart* command. Since the TCP/IP for DOS was customized to use the SLIP interface a connection to the terminal server was established and the local prompt was displayed at our screen.

At this stage we could use our PS/2 to communicate with the services on the networks using TCP/IP over a SLIP interface. For example, we could use Telnet to log in to an RS/6000 which was attached to the Ethernet network.

8.7 Dial-In Connection to Terminal Server

To use a PS/2 running FTTERM V2.1 and a couple of IBM 5853 modems to establish a 2400 bps dial-up connection with the terminal server, we used the following definition for the port on the terminal server:

```
Port 9:  shabani

Character Size:            8         Input Speed:        2400
Flow Control:            XON         Output Speed:       2400
Parity:                 None         Modem Control:   Enabled
Stop Bits:                 2         Profile:
Access:              Dynamic         Local Switch:       None
Backwards Switch:       None         Name:             PORT_9
Break:                 Local         Session Limit:         4
Forwards Switch:        None         Type:               Soft
 XON Char:                 [Q         XOFF Char:            [S
Preferred Service: None
Virtual Login:     None
```

```
Authorized Groups:   0
(Current)  Groups:   0

Enabled Characteristics:

Autobaud,  Autoprompt,  Broadcast,  Input Flow Control,  I/O Flush,
Linemode,  Loss Notification,  Logout Message,  Message Codes,
Output Flow Control,  Verification

Local>
```

Chapter 9. Ethernet Design Considerations

The IBM 8250 Multiprotocol Intelligent Hub will be used both to build new Ethernet networks and to extend existing ones. It is not possible to provide a standard solution for every situation. However, there are a number of rules which must be observed to ensure that the network will operate satisfactorily. This chapter provides a summary of considerations which should be taken into account when an Ethernet network is designed. It also summarizes the design rules when an 8250 is used to build Ethernet networks.

9.1 Ethernet Design Rules

The following is a summary of the considerations that should be taken into account when designing an Ethernet network. But, please note that it is not a complete review of all the design considerations for Ethernet networks as there are many more factors that should be considered when designing local area networks in general and Ethernet LANs in particular.

These considerations for designing Ethernet networks are used to ensure that data transmitted by the source will be received by the destination error free and any collisions that occur can be reliably detected.

1. Maximum segment lengths for each medium type must be exceed the stated limits for that medium:

   - 10BASE-5: 500 m
   - 10BASE-2: 185 m
   - 10BASE-T: 100 m
   - 10BASE-FL: 2000 m
   - 10BASE-FB: 2000 m

   Note that certain products will allow you to go beyond these limits. For example, the 8250 10BASE-T module will allow segments to be longer than 100 m.

   In the case of the 8250 modules, these capabilities are described in Chapter 7, "8250 Ethernet Modules and Accessories" on page 129 wherever applicable.

2. The maximum number of stations allowed on a segment varies according to the type of medium used:

   - 10BASE-5: 100 stations
   - 10BASE-2: 30 stations
   - 10BASE-T: 2 stations
   - 10BASE-FL: 2 stations
   - 10BASE-FB: 2 stations

3. The maximum number of stations in a *collision domain* is 1024.

4. Repeaters can be attached at any position on the *coax segments* but should be at the ends of a *link segment*.

5. Each repeater takes *one* attachment position on the segment and should be counted towards the maximum number of stations allowed on that medium.
6. You can have many segments and repeaters within a single *collision domain* as long as no two DTEs in the same collision domain are separated by more than *four repeaters*.

   Some of the 8250 modules perform a repeater function which should be taken into account when considering the above rule. Table 37 provides a summary of the *repeater presence* of the 8250 modules:

Table 37. 8250 Module's Repeater Presence

8250 Module	**Repeater Presence**
Ethernet Fiber Module	0
Ethernet FOIRL Module	1/2
Ethernet 10BASE-T Module	1/2
Ethernet 50-Pin Module	1/2
Ethernet BNC Module	1
Ethernet Repeater Module	1
Ethernet Transceiver Module	0

7. No two DTEs in the same collision domain can be separated by more than three *coax segments*. The other two segments in a maximum configuration must be *link segments*.
8. *Link segments* can be 10BASE-T, FOIRL, 10BASE-FL and 10BASE-FB.
9. 10BASE-2 and 10BASE-5 segments cannot be used as *link segments*.
10. 10BASE-5 and 10BASE-2, 10BASE-T and fiber segments can be mixed in a single collision domain allowing you to take advantage of the facilities offered by the most appropriate medium for different parts of your network.

9.2 IBM 8250 Multiprotocol Intelligent Hub Ethernet Design Rules and Recommendations

In addition to the above general considerations, we recommend that you adhere to the following rules when designing Ethernet networks using the IBM 8250 Multiprotocol Intelligent Hub.

- Rule 1:

  Wire the backbone in a star topology to simplify fault isolation. A star topology will also provide you with the flexibility needed to cater for the future topology changes brought about due to the requirements of your organization and future technologies.

  It is recommended that you use 62.5/125 fiber cables with ST-type connectors for the backbone (between wiring closets). The drive distances of fiber cable is far in excess of the other supported media. This will enable you to cover the widest physical distance with the LAN. It is also in line with the recommendations that are coming out of the ANSI/IEEE standards organizations.

If you use other media such as UTP for the backbone, the maximum possible distance between transceivers is reduced.

Also it is advisable that you provide extra fiber cables for future needs. The extra cost is (relatively) small compared to potential future benefits.

- Rule 2:

  The maximum fiber Ethernet network span is 4200 meters of fiber cable.

  The 4200 meters is the maximum distance between any two *transceivers* on a pure fiber network.

  The 4200 meters does not include the transceiver cable that connects a device with an external transceiver. The maximum transceiver cable length is 50 meters; thus, total network diameter can be as much as 4300 meters (4200 meters + 2 x 50 meters) between any two nodes connected via external transceivers.

- Rule 3:

  Many LAN products delay the signal that goes through them, resulting in the reduction of the network span. Every microsecond delay shrinks the network diameter by approximately 200 m of fiber cable. The distance reduced by each product is called *equivalent distance*. This factor needs to be taken into account when calculating the *true* span of the network.

  Table 38 gives the equivalent distances (in meters) for various 8250 Ethernet modules.

Table 38. Equivalent Distance Values

LAN Product	**Equivalent Distance**
Ethernet Fiber Module	190
> Incoming signal to Fiber Port	140
> Outgoing signal from Fiber Port	50
Ethernet FOIRL Module	560
> Incoming signal to Fiber Port	330
> Outgoing signal from Fiber Port	230
Ethernet 10BASE-T Module	585
> Incoming signal to 10BASE-T Port	420
> Outgoing signal from 10BASE-T Port	165
Ethernet 50-Pin Module	585
> Incoming signal to TP Port	420
> Outgoing signal from TP Port	165
Ethernet BNC Module	900
> Incoming signal to BNC Port	450
> Outgoing signal from BNC Port	450
Ethernet Repeater Module	800
> Incoming signal to AUI Port	600
> Outgoing signal from AUI Port	200
Ethernet Transceiver Module	0
IEEE Repeater	800

- Rule 4:

  One meter of other media types (such as coax, UTP, etc.) is counted as equivalent of one meter of fiber cable. This is a conservative estimate. For example, the actual equivalence of coax is about 1.1 for each meter of fiber.

- Rule 5:

  The fiber distance between any two devices must not exceed the limits imposed by the optical power budget. This can be affected by:

  - Quality of the fiber cable
  - Existence of patch panels
  - Number of splices on the link
  - Other devices on the network which may be less powerful than the 8250 fiber modules such as transceivers.

  Also, the copper distance between any two devices must not exceed the limits imposed for the interconnected devices. For example, when interconnecting 8250 10BASE-T modules, the distance between them depends on:

  - Type of cable used (STP or UTP)
  - The category of UTP
  - The squelch mode setting of the module

- Rule 6:

  If for any reason you think you may exceed the acceptable network distance, use a bridge to extend the network.

For details about the above rules and examples of their use please refer to *IBM 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide GA33-0191*.

Chapter 10. 8250 Token-Ring Modules and Accessories

This chapter contains descriptions and configuration information about the following modules:

- Token-Ring MAU Module
- Token-Ring Media Module
- Token-Ring Fiber Repeater Module
- Token-Ring Management Module
- Token-Ring Bridge Module
- Token-Ring Accessories

10.1 Token-Ring MAU Module

The token-ring MAU module is a fully compliant 802.5 *Multistation Access Unit (MAU)*. It provides 8 shielded RJ-45 ports for connecting workstations via UTP or STP to token-ring networks operating at 4 or 16 Mbps.

The token-ring MAU module provides RI/RO ports which support connection to other token-ring MAU modules, to token-ring management modules and to token-ring fiber repeater modules, on the same or different 8250 as well as connection to other 802.5 compliant MAUs such as the IBM 8228 Multistation Access Unit and IBM 8230 Controlled Access Unit. When connecting two or more token-ring MAU modules together, each one can support UTP or STP lobe cables independent of the other.

The 8-port token-ring MAU module occupies one slot on the 8250. This allows you to have a maximum of 16 token-ring MAU modules installed in a single 8250 Model 017 and 6 Modules in an 8250 Models 006 or 6HC.

10.1.1 MAU Module Features

The token-ring MAU module provides a special feature called *RI/RO Cable Monitor Mode* which can be used when connecting two or more token-ring MAU modules within the same 8250. The cable monitor mode is also supported on the copper RI/RO ports of the token-ring management module and the token-ring fiber repeater module. When enabled, this feature will detect any fault on the cable between the connected modules and will automatically wrap the ports causing the backup path to be used to keep the network running.

Figure 100 on page 210 shows the normal and the wrapped operation of the RI/RO cable monitor mode feature in a configuration of three MAU modules. In the example, called *wrapped operation*, the cable between the middle and the right-most module is broken. The main and the backup ring are automatically wrapped at the ports connected to the *faulty* cable, resulting in the isolation of this faulty cable.

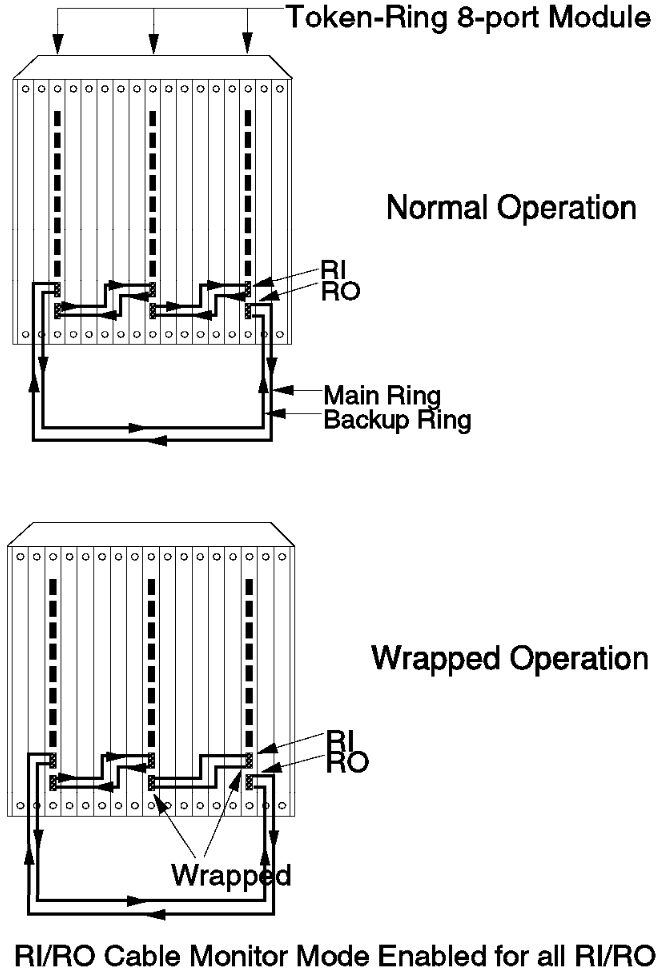


Figure 100. RI/RO Cable Monitor Feature

To take advantage of this feature, you must use the special 8-pin RJ-45 cable supplied with the MAU module to connect the two modules. This cable is 10 inches in length. You will need a longer cable if the the two modules being interconnected are not within four slots of one another. You can order a longer cable, up to 30 inches long, separately. See also 10.6, “Token-Ring Accessories” on page 254 for more details.

The cable monitor mode must be disabled when the token-ring MAU module is connected to the IBM 8228 and IBM 8230. Also, this feature may be used between modules installed on two different 8250s, only if it can be guaranteed that both 8250s will have the same *ground potential*.

Note that this feature can be enabled/disabled for RI and RO independently.

The token-ring MAU module provides a facility called *bypass mode*. The bypass mode allows you to isolate all the ports on the module, while its RI/RO ports remain in the ring and will pass network data to the other MAUs to which it is connected. To set this facility requires the use of a management module.

If a management module is present in the box when you install the MAU module, the module comes up in bypass mode.

If no management module is present in the 8250, the module disables bypass mode automatically so that its lobe ports will communicate with the stations on the ring to which the module is connected.

Like all other 8250 modules, the token-ring MAU module can be installed/removed without powering off the 8250.

10.1.2 Connection to Other MAUs

The 8-port token-ring MAU module can be connected to MAU modules in other concentrators or to any other 802.5 compliant Multistation Access Unit such as the IBM 8228 or IBM 8230. This is shown in Figure 101 on page 212.

When the MAU module is connected to the other MAUs, the setting of the cable monitor mode is of particular importance. This feature *must* be disabled when the module is connected to the modules in another 8250 (unless the same ground potential can be guaranteed) or other MAUs such as the IBM 8228 or IBM 8230. Please note the setting of the cable monitor mode, in Figure 101 on page 212.

Note

If you enable the cable monitor mode for an RI/RO connection to another device which does not support this feature (such as an IBM 8228), the MAU module will automatically wrap that port both internally and externally.

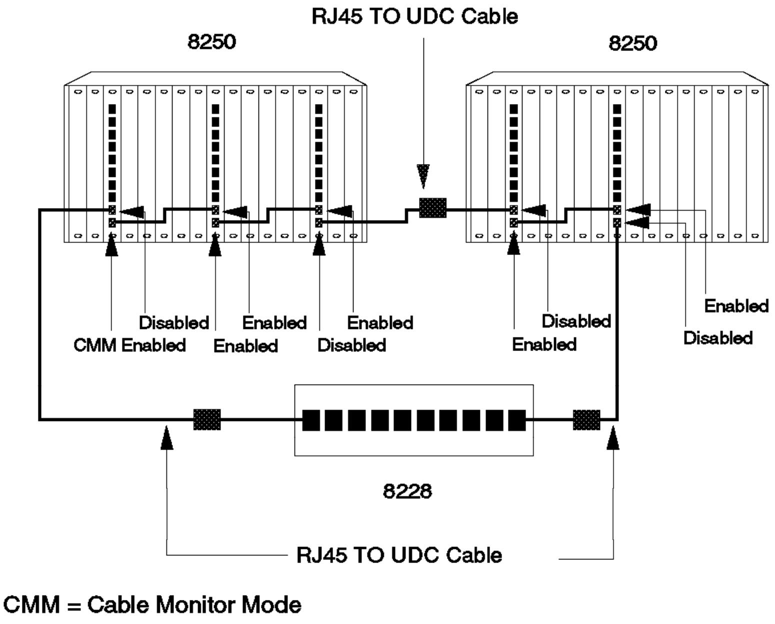


Figure 101. Connection to Other MAUs

To connect the MAU module to other modules in another 8250, or to other MAUs, using the IBM cabling system, you must use an RJ-45 to IBM Universal Data Connector cable. The pinout used by this cable is given in Table 39.

Table 39. Shielded RJ-45 to UDC Connector

RJ-45 Pin	UDC Pin Color	Pin Function
3	Black	Station Transmit
4	Red	Station Receive
5	Green	Station Receive
6	Orange	Station Transmit
Shield		Shield

10.1.3 STP and UTP Limitations

The following are the limitations when you use *STP* cables with the MAU module:

- Max 260 stations on 4 Mbps.
- Max 132 stations on 16 Mbps.
- 385 m max lobe length at 4 Mbps in a single wiring closet.
- 173 m max lobe length at 16 Mbps in a single wiring closet.
- 100 m lobe length is recommended.

The following are the limitations when you use *UTP* cables with the MAU module:

- UTP categories 3, 4 and 5 are supported at 4 Mbps.
- UTP categories 4 and 5 are supported at 16 Mbps.
- Max 72 stations on 4 Mbps (UTP-3/4/5).
- Max 132 stations on 16 Mbps (UTP-4/5).
- 100 m max lobe length.
- UTP Media Filter is required for both 4 and 16 Mbps.

More detailed information can be found in the *IBM 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide (GA33-0191)*.

10.1.4 Front View and LED Description

The token-ring MAU module has 10 LEDs on the front panel that indicate the state of the module. Figure 102 shows the location of these indicators and Table 40 describes what these indicators mean.

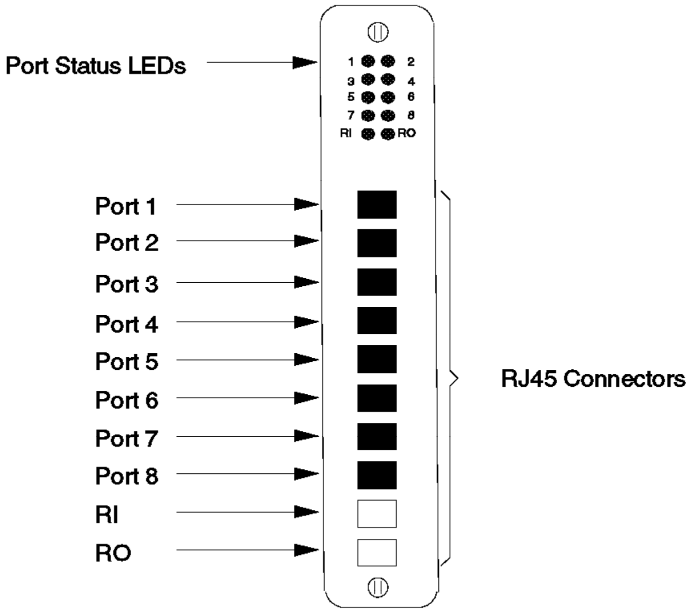


Figure 102. Front View of the TR MAU Module

Table 40 (Page 1 of 2). MAU LED Descriptions

LED name	Color	State	Description
Port Status	Green	OFF	Port disabled.
		ON	Port enabled and inserted into the ring
		Blinking	Port enabled but not inserted.

Table 40 (Page 2 of 2). MAU LED Descriptions

LED name	Color	State	Description
RI/RO Status	Green	OFF	Trunk disabled.
		ON	Trunk enabled and functioning.
		1 Blink	Trunk enabled and cable fault detected.
		2 Blinks	Trunk enabled and intermittent activity detected.

Figure 103 shows the token-ring MAU module dip switches and jumpers, their meanings and the factory settings.

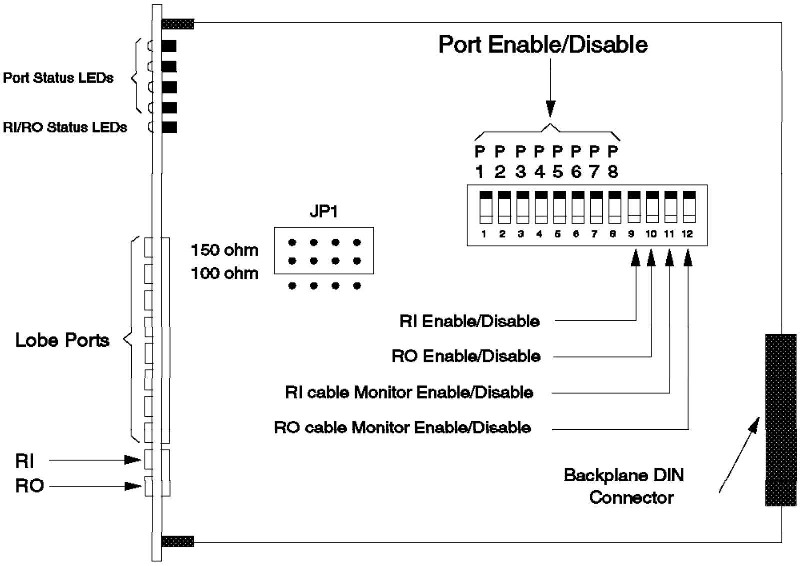


Figure 103. Side View of the TR MAU Module

10.1.5 Configuring Token-Ring MAU Module

To configure a token-ring MAU module, you must do the following:

- Enable/disable ports

  This can be done using the onboard dip switches or the following management module command:

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

  Note that each port can be enabled/disabled independently from the other ports.

- Select UTP or STP cabling

The impedance on the module should be set to correspond with the type of twisted pair which is used on the lobe cable. For UTP, the impedance should be set to 100 ohms and for STP to 150 ohms.

The impedance must be set via onboard jumpers before you install the module. You cannot override this through the management commands.

Also, the RI/RO ports are always set to 150 ohm impedance regardless of the jumper position.

All the cables attached to the module must be consistent with the impedance setting. This means that you should not mix UTP and STP cables on the same module. However, different interconnected MAU modules can using different lobe cables.

- Enable/disable RI/RO ports

  You can do this by using the onboard dip switches or the following management module command:

  ```
  SET TRUNK {slot} RING_IN/RING_OUT MODE {enable/disable}
  ```

  The RI/RO ports can be enabled/disabled independently.

- Enable/disable RI/RO cable monitor mode

  You can do this by using the onboard dip switches or the following management module command:

  ```
  SET TRUNK {slot} RING_IN/RING_OUT CABLE_MONITOR {enable/disable}
  ```

- Set bypass mode

  You can do this only through the following management module command:

  ```
  SET module {slot} MODE {bypass/insert}
  ```

10.2 Token-Ring Media Module

The token-ring media module (also called 20-port token-ring module) provides 20 shielded RJ-45 ports for connecting workstations via unshielded twisted pair (UTP) or shielded twisted pair (STP) to token-ring networks operating at 4 or 16 Mbps. While mixing different media cables on the same module is not allowed, different modules on the same ring can use different types of lobe cables.

The token-ring media module occupies two slots on the 8250.

10.2.1 TR Media Module Features

The token-ring media module contains an *integrated repeater* which is on the path from the backplane to the ports on the module. When the repeater is connected to one of the token-ring networks on the backplane, the repeater will regenerate the signal received over the backplane before passing it to the ports on the module.

> **Note**
>
> Signal enters the token-ring media module at port 20 and exits at port 1.

This repeater does not have a MAC address and does not take part in the token-passing protocol. It only re-times and regenerates the signal passing through it.

In a *managed environment* (when at least one management module is present) you can install up to a maximum of seven token-ring media modules. These modules can all be connected to a single token-ring network providing you with a total of 140 token-ring ports in a single 8250. Alternatively, they can be connected to one of the seven different token-ring networks (the maximum number of token-rings supported on a single 8250 when no other protocol is used) to form up to a maximum of seven token-ring networks on a single 8250.

You can install up to two token-ring media modules on a managed 8250 Model 6 or 6HC for a total of 40 ports.

You can also set any module to be isolated, enabling you to set up isolated networks, each with 20 ports.

In an *unmanaged environment* you can install up to a maximum of eight token-ring media modules on a single 8250 Model 017, allowing you to have up to a maximum of 160 ports on a single 8250. However, note that the module occupying either of the 16th or 17th slot will always be isolated and unable to communicate with the other modules.

You can install up to three token-ring media modules on an unmanaged 8250 Model 6HC for a total of 60 ports and two media modules on the Model 006.

In an unmanaged environment, there can be one or three token-ring networks on the 8250 Model 17 and one or two token-ring networks on an 8250 Model 006 or 6HC. The token-ring media modules can attach to any one of these rings or be set isolated depending on the 8250 slot that the module is installed on. See 10.2.5, “Unmanaged 8250 Considerations” on page 219 for more information.

The token-ring media module contains built-in *automatic wrap capability* on the twisted pair lobe ports. This provides a bypass of the port in the event of a lobe cable or station failure. The module also provides automatic reconnection to the network when the break in the lobe cable is repaired.

The token-ring media module can be managed via any of the three types of management modules available on the 8250. It can also be managed via an SNMP manager such as AIX NetView Management Program/6000, using the SNMP agent function provided by the management modules.

10.2.2 STP and UTP Limitations

The following are the limitations when you use *STP* cables with the media module:

- Max 260 stations on 4 or 16 Mbps.
- 375 m max lobe length at 4 Mbps in a single wiring closet.
- 145 m max lobe length at 16 Mbps in a single wiring closet.
- 100 m lobe length is recommended.

The following are the limitations when you use *UTP* cables with the media module:

- UTP categories 3, 4 and 5 are supported at 4 Mbps.
- UTP categories 4 and 5 are supported at 16 Mbps.
- Max 72 stations on 4 Mbps (UTP-3/4/5).

- Max 132 stations on 16 Mbps (UTP-4/5).
- 100 m max lobe length.
- UTP media filter is required for both 4 and 16 Mbps.

10.2.3 Front View and LED Description

The token-ring media module has 21 LEDs on the front panel that indicate the state of the module and its ports. Figure 104 shows the location of these indicators and Table 41 describes what these indicators mean.

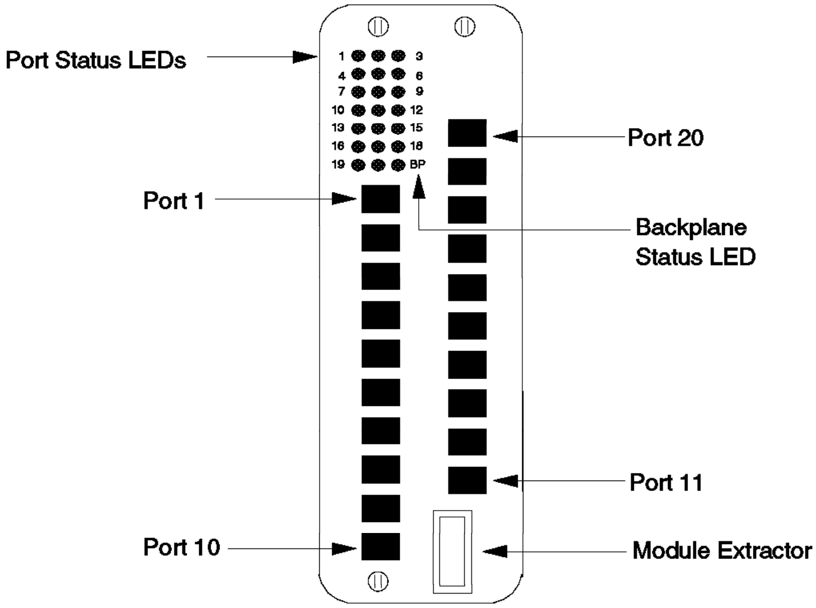


Figure 104. Front View of the TR Media Module

Table 41 (Page 1 of 2). TR Media Module LED Descriptions

LED name	State	Description
Port Status 1-20	OFF	Port disabled.
	ON	Port enabled and functioning properly.
	1 blink	No station detected (that is, no phantom current present) and port is enabled. This condition causes the signal to wrap automatically.

Table 41 (Page 2 of 2). TR Media Module LED Descriptions

LED name	State	Description
Backplane Status	OFF	Module is isolated from the backplane and is operating without error.
	ON	Module is operating on the backplane without error.
	1 blink	Module is operating on the backplane, but its configuration has changed as a result of an error recovery.
	2 blinks	A frequency acquisition error has occurred on the module.
	3 blinks	A hardware error is detected on the module and has resulted in the module shutting down.

Figure 105 shows the token-ring media module dip switches and jumpers.

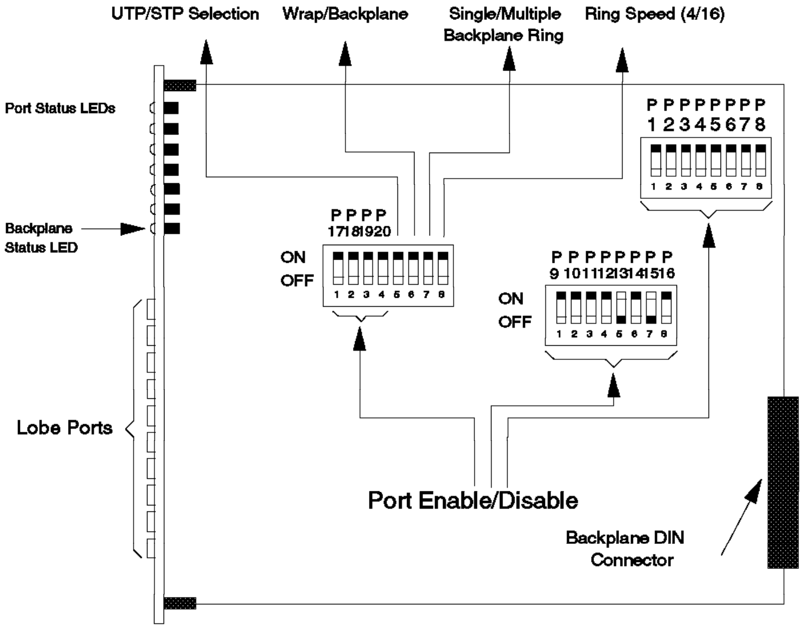


Figure 105. Side View of The TR Media Module

10.2.4 Configuring Token-Ring Media Module

To configure the token-ring media module, you must do the following:

- Assign the module to a network

  In a managed environment, this can be done via the following command:

  ```
  SET MODULE {slot} NETWORK {network}
  ```

For network assignment in an unmanaged environment, refer to 10.2.5, “Unmanaged 8250 Considerations” on page 219.

- Enable/disable the ports

  This can be done via onboard dip switches or the following management module command:

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

  Each port can be enabled/disabled independently from the other ports.

- Select STP or UTP cabling for the lobes

  This can be done via onboard dip switches or the following management module command:

  ```
  SET MODULE {slot} CABLE_IMPEDANCE {100/150ohm}
  ```

  The impedance on the module should be set to correspond with the type of twisted pair which is used on the lobe cable. For UTP, the impedance should be set to 100 ohms and for STP to 150 ohms.

  All the cables attached to the module must be consistent with the impedance setting. This means that you mix UTP and STP cables on the same module.

- Set the ring speed

  Setting the module to operate at 4 or 16 Mbps can be done via onboard dip switches or the following management module command:

  ```
  SET MODULE {slot} RING_SPEED {4/16mbps}
  ```

10.2.5 Unmanaged 8250 Considerations

In an unmanaged environment, you must use the *wrap/backplane* dip switch to enable communication over the backplane. If this is not enabled, the module will be isolated.

When you enable the wrap/backplane dip switch, you will be able to use the backplane to form a token-ring network consisting of this module and the other token-ring modules which are enabled to communicate over the backplane.

Additionally, to set up token-ring networks using the backplane, the token-ring modules must also be set to allow a single ring or multiple rings (three in the Model 017 and two in the Model 006 and 6HC) via setting the *single/multiple backplane ring* dip switch to the OFF or ON position, respectively.

Note

All the modules within the same 8250 must have identical settings for single/multiple rings; otherwise unpredictable results can happen.

If the modules are set to one ring, all the modules in the 8250 which are enabled to use the backplane are configured to operate on the same backplane ring.

If the modules are set to operate in multiple backplane ring mode, the slot in which a module resides determines the ring to which the module is attached.

In an unmanaged environment, when the backplane is enabled (via the wrap/backplane dip switch of a module already installed on the 8250), a new module that is inserted into the 8250 will not be recognized by the other modules on the backplane until you force a backplane reinitialization. To force a backplane reinitialization, you must perform the following steps:

1. Press the LED check button once. All of the module′s LEDs will light.
2. Immediately after pressing the button, press it again twice within one second.

A clicking sound will indicate that the reinitialization of the backplane has occurred.

If a module failure should occur in an unmanaged 8250, you must use the above procedure to reinitialize the module once the problem has been fixed.

To summarize the above points, in an unmanaged 8250, the following points should be taken into consideration:

1. The setting of the wrap/backplane dip switch will determine if the module is to be assigned to a ring on the backplane or set to isolated mode.
2. You can have one or three rings on a Model 017 and one or two rings on a Model 006/6HC. The choice between a single or multiple rings on the backplane is made through the single/multiple dip switch on the module. To have multiple rings, all the modules should be set to multiple ring mode.
3. Up to a maximum of eight token-ring media modules can be installed in an unmanaged Model 017. However, the module occupying slot 16 or 17 will always be isolated from the other modules regardless.
4. Up to a maximum of three token-ring media modules can be installed in an unmanaged 8250 Model 6HC (two in the case of Model 006).

The assignment of a module to a ring is determined by the slot position occupied by the token-ring media module. These dependencies are shown in Table 42 for the 8250 Model 017 and in Table 43 for 8250 Model 006/6HC.

Note that a token-ring media module is a two-card module and the right-most card determines the position of the module.

Table 42. Ring/Slot Assignment for 8250 Model 017

Ring Number	Slot Assignment
One	1, 2, and 3
Two	4 through 9
Three	10 through 15
Isolated	16 and 17

Table 43. Ring/Slot Assignment for 8250 Model 006/6HC

Ring Number	Slot Assignment
One	1, 2, and 3
Two	4, 5, and 6

10.2.6 Configuration Example

Figure 106 shows an example of using 8250 token-ring media modules. In this example, two of the modules have been assigned to ring 1, enabling the workstations attached to these modules to use the 8250 backplane to communicate with each other. Note that in this managed 8250, the token-ring media modules do not need to be adjacent to each other to form a single ring.

The third module has been set to isolated mode creating a separate ring. The workstations attached to this module can only communicate with each other.

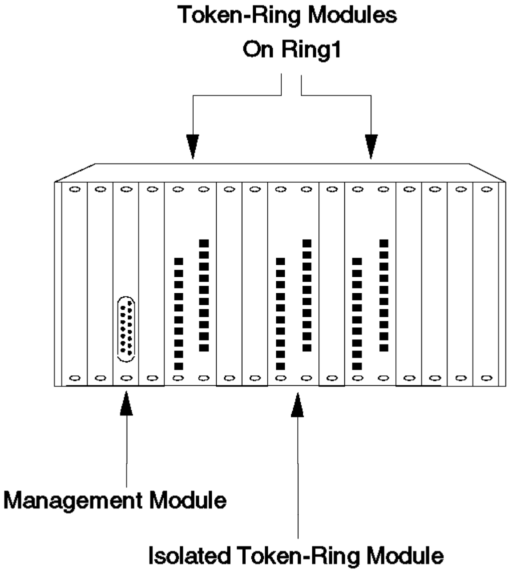


Figure 106. Configuration Example Using TR Media Module

10.3 Token-Ring Fiber Repeater Module

The token-ring fiber repeater module is a single-slot module which allows you to:

1. Interconnect 8250s over fiber and/or copper (only STP) cables.
2. Connect an 8250 over fiber to an IBM 8230.
3. Connect an 8250 to another concentrator such as IBM 8228 or IBM 8230 over STP cables.
4. Connect to the token-ring management module over copper cables.

This module can be connected to one of the seven internally established token-ring networks via the backplane, or can be set to isolated mode. When connected to the backplane, it can communicate with other token-ring modules (such as the 20-port module or token-ring management module) which support the backplane interface.

Note

To connect to an IBM 8230 over fiber, the *compatibility mode* for that trunk must be set to ON. More information is provided later in this section.

The token-ring fiber repeater module supports networks operating at 4 or 16 Mbps.

For fiber connections, this module provides a pair of fully repeated fiber RI/RO ports with ST connectors. The following fiber types are supported:

- 62.5/125
- 50/100
- 85/125
- 100/140

The fiber repeater module provides three physical repeaters. The repeater functions are performed over the fiber main path, the fiber backup path and the backplane interface. This allows you to extend the distance between concentrators to a maximum of two kilometers over the 62.5/125 fiber cable.

This module also provides a pair of non-repeated copper RJ-45 RI/RO ports for interconnecting to the following:

- 8-port token-ring MAU modules in the same or a different 8250
- Other fiber repeater modules in the same or a different 8250
- IBM 8228 Multistation Access Unit
- IBM 8230 Controlled Access Unit
- 8250 token-ring management module

Note that this type of connection must be done over STP cables.

The fiber repeater module also contains two RJ-45 lobe ports which can be used to attach token-ring stations. A common application for these ports will be connection to bridges, routers and servers. These ports can be set via jumpers to UTP or STP individually.

10.3.1 Features

The fiber repeater module is able to automatically wrap the network signal on the fiber cables onto the backup path when there is a network failure, such as a break in the fiber cable. This module can also sense when a cable break has been repaired and automatically switch the data back to the main path.

The fiber repeater module also provides fault detection and recovery over the copper RI/RO ports. This is achieved through the use of *squelch detection* and *cable monitor mode*. The cable monitor mode is described in 10.1.1, “MAU Module Features” on page 209.

The fiber repeater module can be connected to any of the seven (three in an unmanaged Model 017 and two in an unmanaged Model 006/6HC) internal token-ring networks on the backplane or can be set to isolated mode.

The fiber repeater module can be managed using any of the 8250 network management modules.

10.3.2 Front View and LED Description

The fiber repeater module has seven LEDs on the front panel that indicate the status of each port and trunk. Figure 107 shows the location of these indicators and Table 44 describes what these indicators mean.

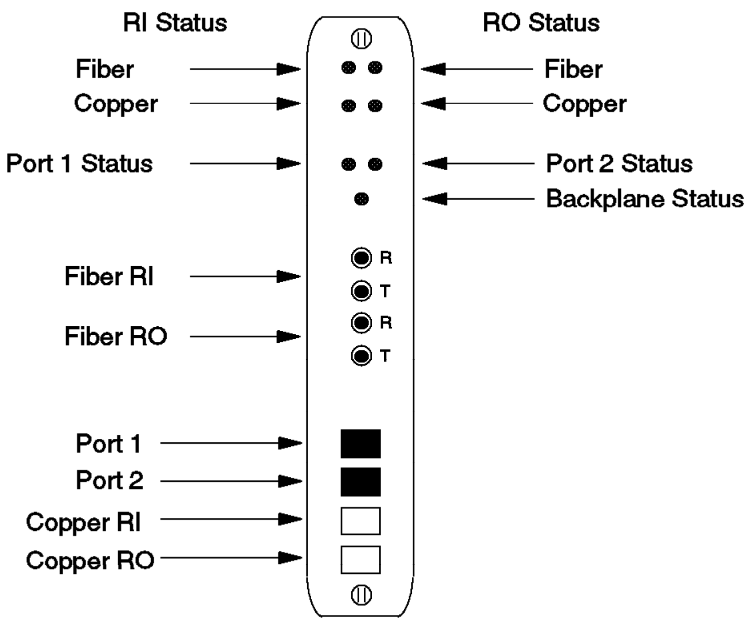


Figure 107. Front View of the TR Fiber Repeater Module

Table 44 (Page 1 of 2). TR Fiber Repeater LED Descriptions

LED name	State	Description
Fiber RI/RO	OFF	Port disabled.
	ON	Port enabled and functioning.
	1 Blink	Port enabled but no light detected.
	2 Blinks	Signal frequency acquisition error on the port (valid for RO when the backup path is not used).
	3 Blinks	Hardware error detected on the port.
Copper RI/RO	OFF	Port is disabled.
	ON	Port enabled and functioning.
	2 Blinks	Squelch error detected.
Lobe Port 1 & 2	OFF	Port is disabled.
	ON	Port enabled and functioning.
	1 Blink	No station detected on the port.

Table 44 (Page 2 of 2). TR Fiber Repeater LED Descriptions

LED name	State	Description
Backplane	OFF	Module is isolated.
	ON	Module is operating on the backplane.
	1 Blink	Module is operating on the backplane, but its configuration has changed as a result of an error recovery.
	2 Blinks	A frequency acquisition error has occurred on the module.
	3 Blinks	A hardware error detected on the module has resulted in the module shutdown.

Note that a frequency acquisition error (indicated by the LED blinking twice) may be the result of the phase lock loops not successfully remaining locked. This may occur when there are no stations on the network path and the phase lock loop does not have any data to lock onto. This condition may occur frequently on the fiber RO trunk if the backup path is not used. This should not be considered a problem. However, if stations are attached and a frequency acquisition error occurs on the main path, the condition should be treated as an error and may be the result of an improperly configured ring speed setting.

Figure 108 shows the token-ring fiber repeater module dip switches, their meanings and the factory settings.

Please note that the jumpers (JP1 and JP2) and the unused dip switches are factory set to desired positions. Please do not change these settings.

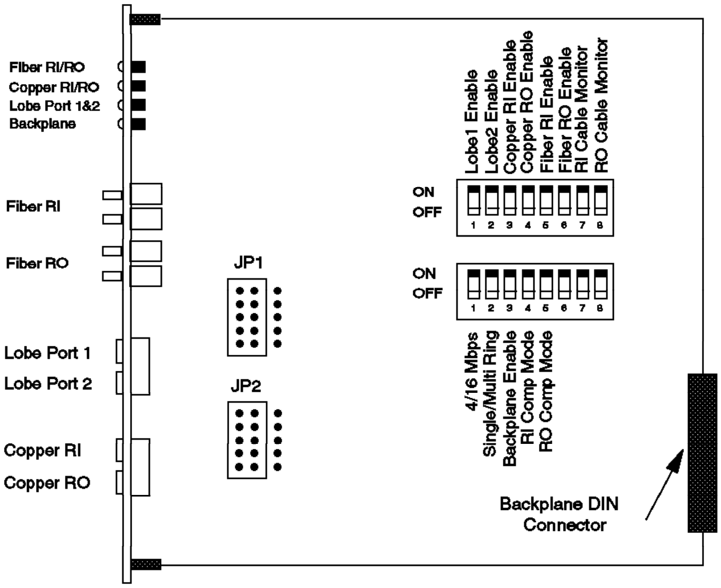


Figure 108. Side View of the TR Fiber Repeater Module

10.3.3 TR Fiber Repeater Module Data Path

The following figures: Figure 109, Figure 110 on page 226, Figure 111 on page 226, Figure 112 on page 227 and Figure 113 on page 227 show the data path of the token-ring fiber repeater module.

Please note the location of the repeaters on the data path. These repeaters have no MAC address and only re-time and regenerate the signal. They do not take part in any token-ring protocol.

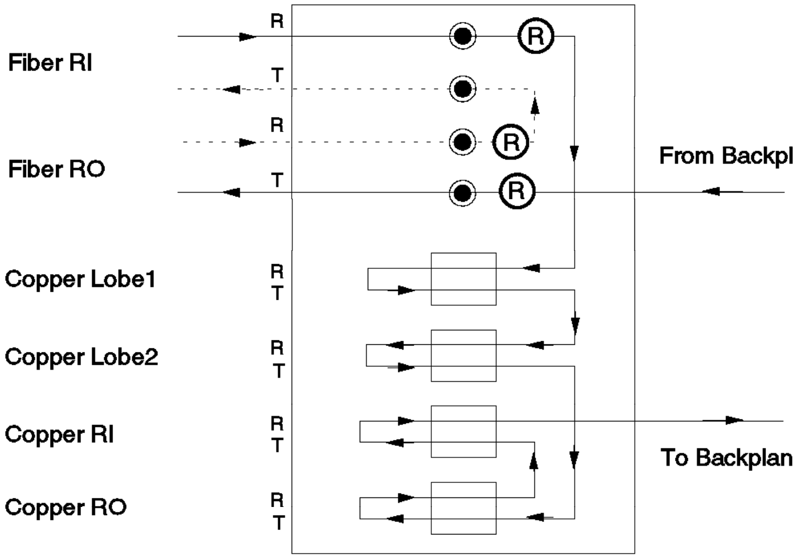


Figure 109. Using TR Fiber RI/RO Ports Only

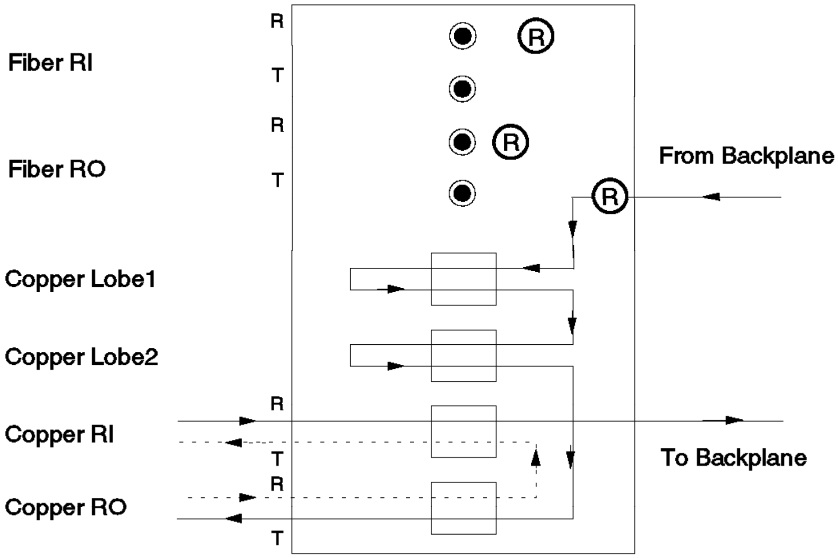


Figure 110. Using TR Copper RI/RO Ports Only

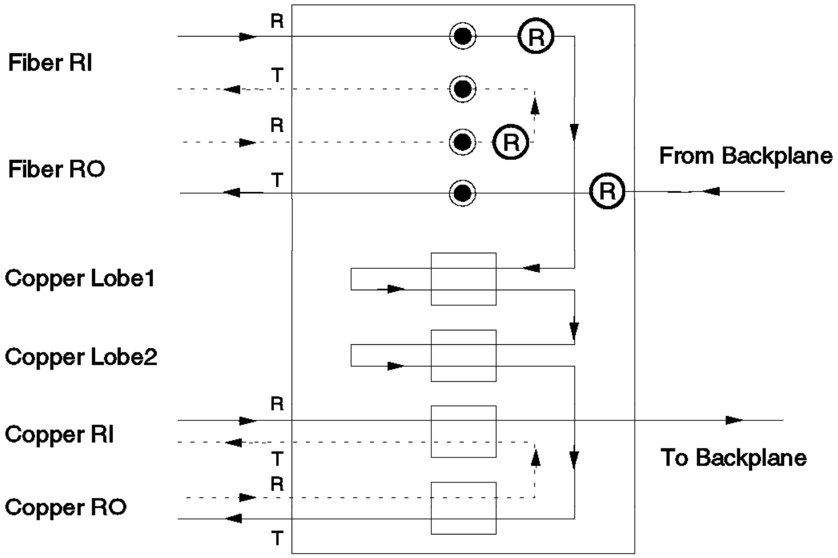


Figure 111. Using TR Fiber and Copper RI/RO Ports

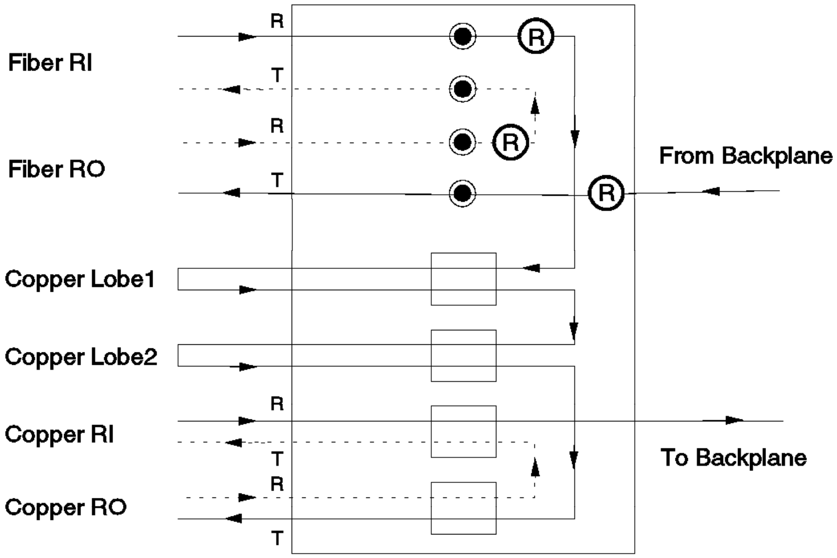


Figure 112. Using all the TR Repeater Ports

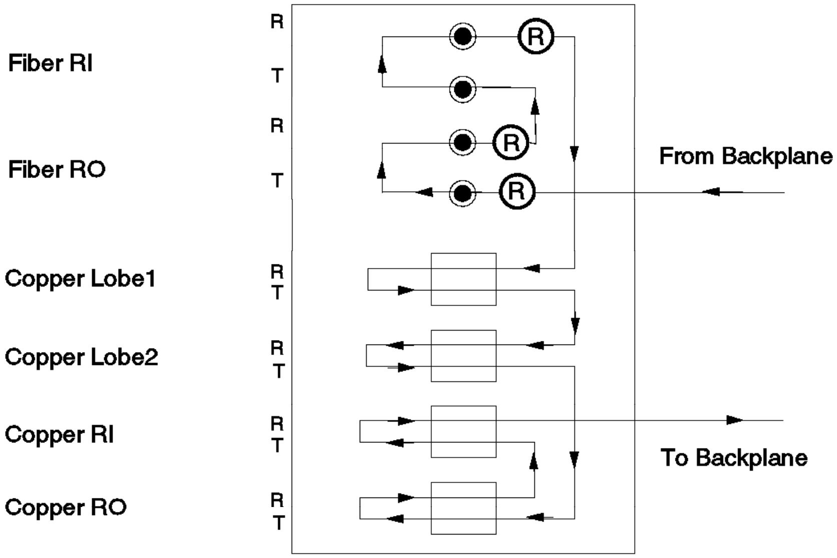


Figure 113. Copper and Fiber in Wrapped State

10.3.4 Network Segmentation

If two fiber repeater modules are connected using both the fiber RI/RO and the copper RI/RO trunks simultaneously, the network will be segmented into two distinct rings. Figure 114 shows the two rings which will be formed in such a case. Therefore, you should avoid using such a configuration.

The segmentation will occur if the two modules are located in two different 8250s or on a single 8250 but are attached to different backplane networks.

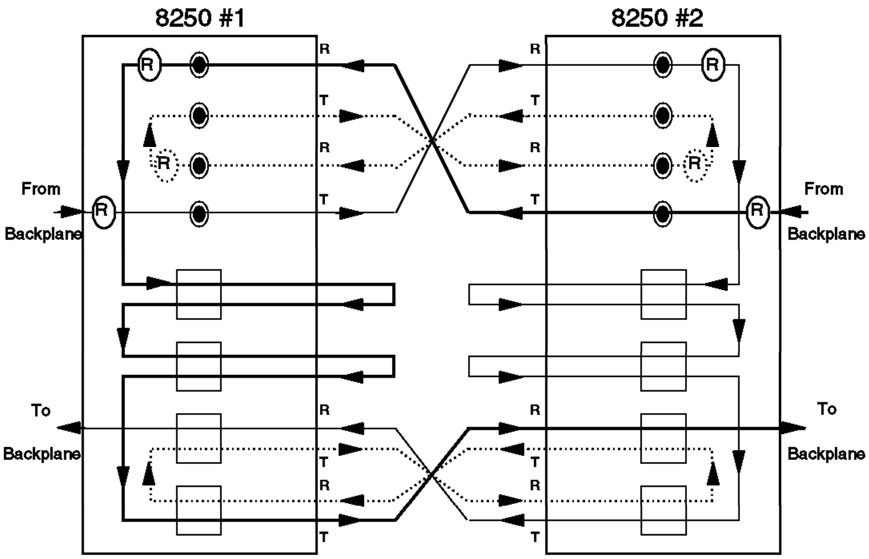


Figure 114. Network Segmentation. Two modules are connected using both copper and fiber trunks.

Also, if you connect two fiber repeater modules (via fiber or copper trunks) that are attached to the same backplane token-ring network, the network will be segmented into two distinct rings.

Figure 115 on page 229 shows the two distinct rings which are formed if we try to connect two fiber repeater modules via fiber trunks, while the two modules are connected to the same 8250 backplane network.

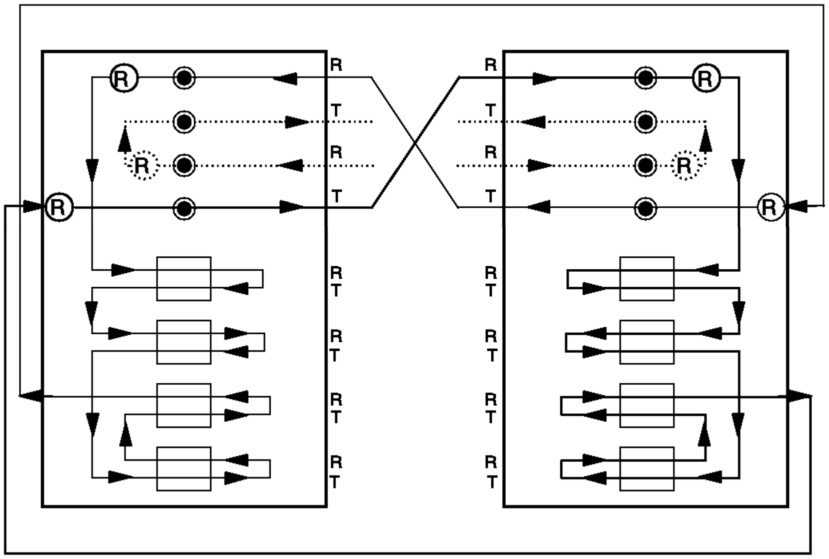


Figure 115. Network Segmentation. Two modules are in the same 8250.

To test the above scenario, we first configured an 8250 with the following configuration:

```
Slot  Module       Version Network       General Information
----  ------------ ------- ------------- -------------------
 01   C00NS-RCTL   001     N/A           Active Controller Module
 02   C00NS-RCTL   001     N/A           Standby Controller Module
 03   T02MS-FIB    001     TOKEN_RING_1  Port(s) are down
*05   T01MS-MGT    v1.11-B TOKEN_RING_1  Master Management Module
 06   T02MS-FIB    001     TOKEN_RING_1  Port(s) are down
```

As can be seen, modules 3 and 6 are fiber repeater modules and module 5 is a token-ring management module. We connected a station to port 1 of the module 3 and a LNM to port 1 of the module 6. When we had no fiber or copper cables between the two fiber repeater modules, the LNM showed three stations on the LAN segment. These were:

- LNM attached to port 6.1
- MAC address of TRMM
- Station attached to port 3.1

We also did a display of the *logical token-ring* using the following TRMM command:

```
show network_map token-ring logical
```

The result of the display was as follows:

```
Token Ring Logical Map
  MAC Address           Slot     Port
  -----------------     ----     ----
  10-00-f1-0f-09-5c     5        1
  40-00-00-03-33-16     6        1
  10-00-5a-4d-06-24     3        1
```

Then we connected the two fiber repeater modules using a pair of fiber cables. At this stage, LNM showed its segment containing only one station (LNM itself) and the output from TRMM *show network_map token_ring logical* command showed another segment containing the following two stations:

```
Token Ring Logical Map
  MAC Address          Slot     Port
  -----------------    ----     ----
  10-00-f1-0f-09-5c    5        1
  10-00-5a-4d-06-24    3        1
```

This experiment confirmed the existence of two distinct rings when two fiber repeater modules are connected to the same backplane network as well as being connected via fiber or copper trunks.

10.3.5 Using Fiber and Copper in the Same Segment

If you are planning to have both copper and fiber between the hubs within a single ring, you must ensure that:

1. The copper connections form a complete physical ring and

2. The fiber connections form a complete physical ring

This will ensure that your whole network is a single logical ring. For example, Figure 116 on page 231 shows two fiber connections from one 8250 to another 8250 and two copper connections from this 8250 to a third one. This is a valid example for using fiber and copper in the same segment. This is because there are two complete physical rings (one fiber and one copper) which form a single logical token-ring network. If you follow the data path, you can see that the backplane and all copper lobes are on the same ring.

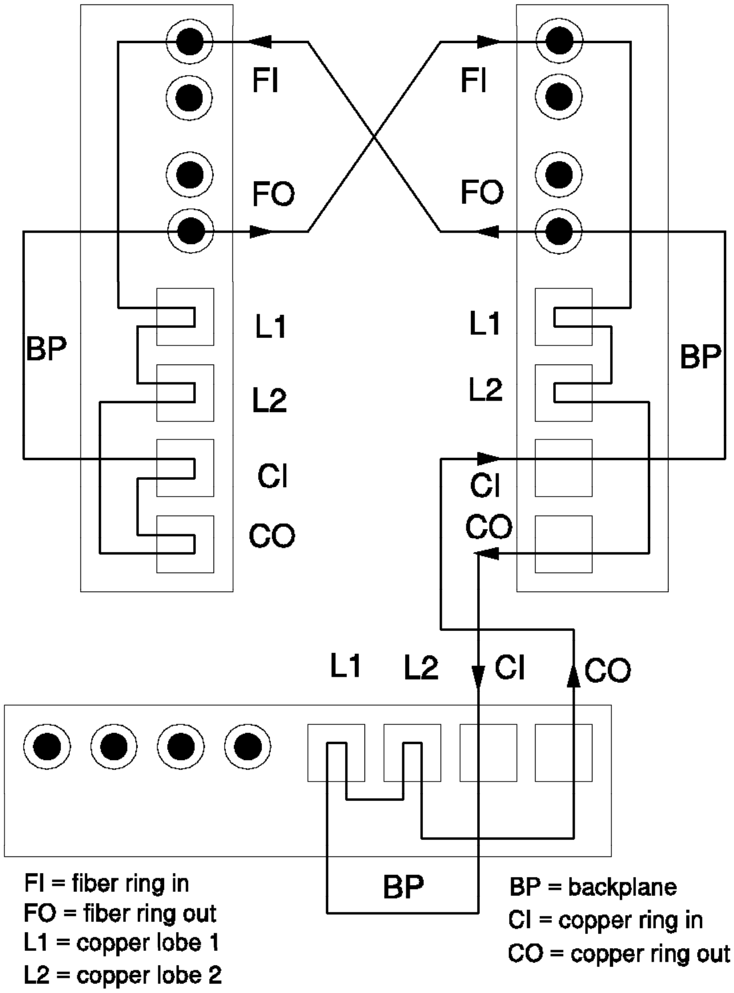


Figure 116. Valid Mixed Fiber and Copper Configuration

However, if you mix copper and fiber so that your physical rings are a mixture of fiber and copper, your network will be segmented into two distinct token-ring networks.

Figure 117 on page 232 shows an example of invalid usage of fiber and copper in the same segment. In this case, there is one copper cable connected from concentrator #3 to #1 and another from #3 to #2 while #1 and #2 are connected to each other via a fiber cable. This leads to a fragmentation of the network into two distinct segments. The first segment consists of #1′s backplane, the copper lobes of #2 and #3′s backplane. The second segment consists of #1′s copper lobes and the backplane of #2.

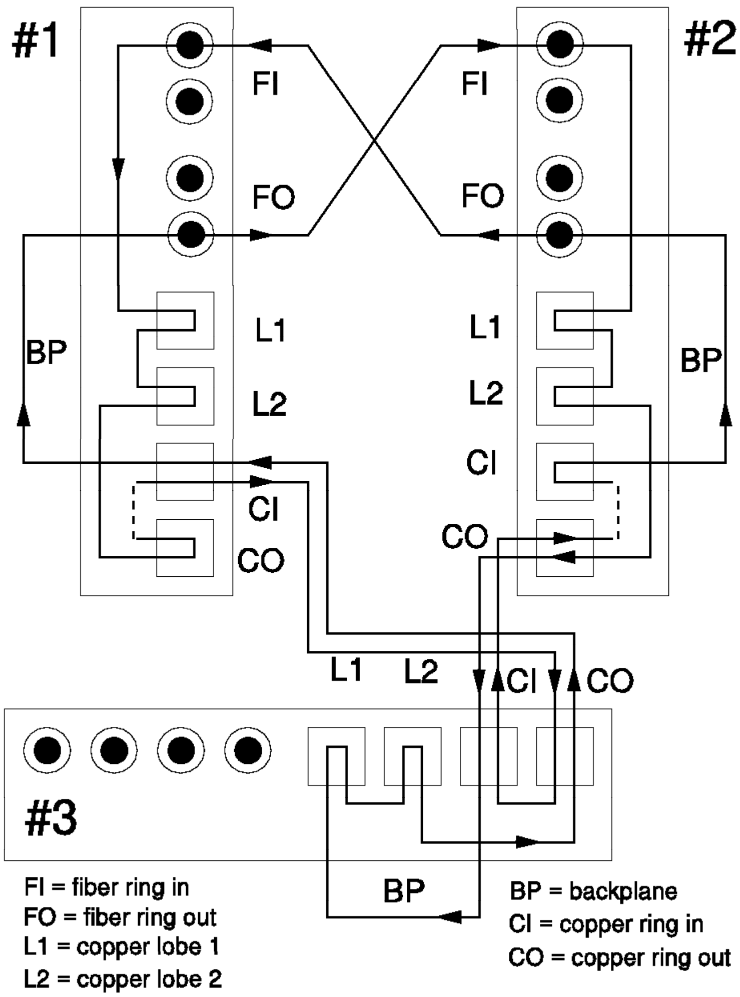


Figure 117. Invalid Mixed Fiber and Copper Configuration. Segment is fragmented into two rings.

As mentioned earlier, the 8250 can be connected to an IBM 8230 in a so-called compatibility mode. The connection is either done with fiber or with copper. If you are using copper and fiber in one segment, the same rules apply. A valid configuration is shown in Figure 118 on page 233.

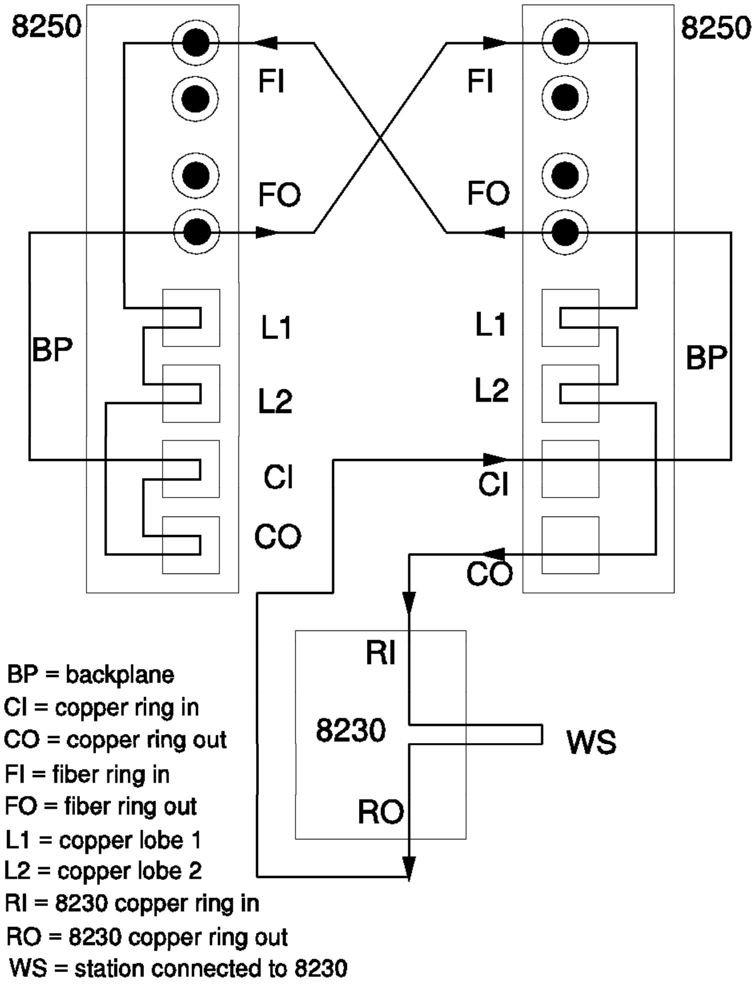


Figure 118. Valid 8230/8250 Configuration

An example of an invalid configuration is given in Figure 119 on page 234 where the RO of the 8230 is connected to the RI of the 8250 #1 and RI of the same 8230 is connected to the RO of 8250 #2. This configuration will result in a fragmented network consisting of two distinct rings. As can be seen, one ring consists of 8250 #1′s backplane, 8250 #2′s copper lobes and the stations connected to the 8230. The other ring consists of 8250 #2′s backplane and 8250 #1′s copper lobes.

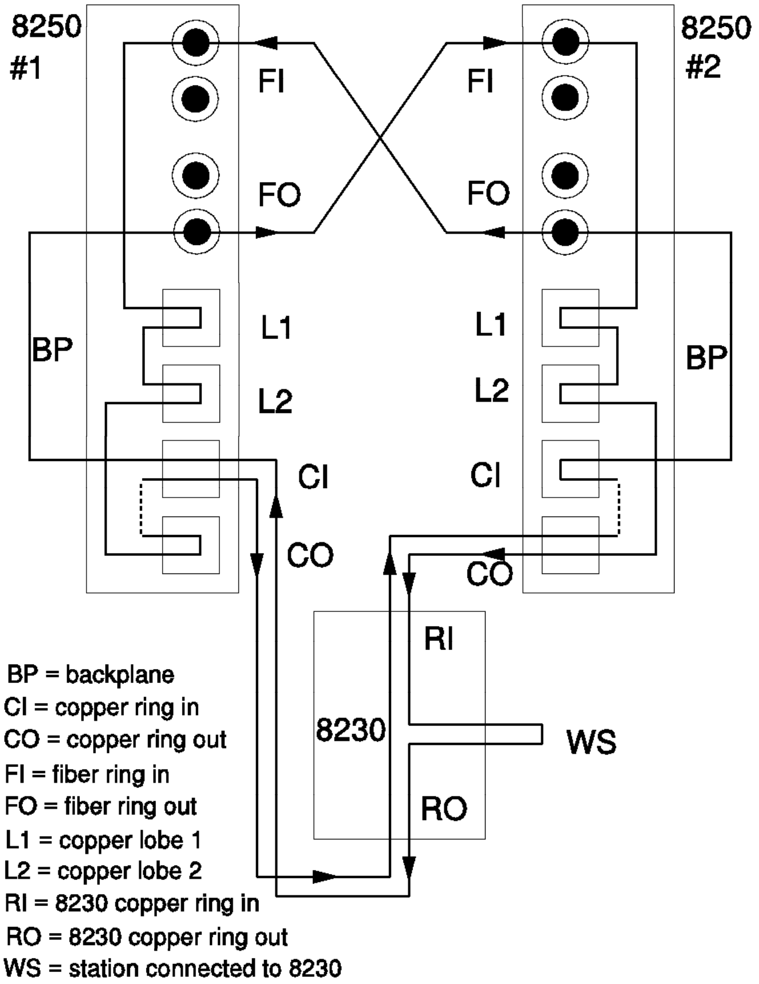


Figure 119. Invalid 8230/8250 Configuration. Segment is fragmented into two rings.

10.3.6 Recovery between TR Fiber Repeater and 8230

If you connect an IBM 8230 to an IBM 8250 using fiber, there are six possible types of link failure as shown in Figure 120 on page 235.

The hardware on the fiber repeater module will allow wrapping in the following four cases:

1. Break #1 is break between 8230 RO and 8250 RI on the primary ring. The 8230 will wrap RO and the 8250 will wrap RI.
2. Break #2 is break between 8230 RO and 8250 RI on both the primary and the secondary path. The 8230 will wrap RO and the 8250 will wrap RI.
3. Break #3 is break between 8250 RO and 8230 RI on the secondary ring. The 8230 will wrap RI and the 8250 will wrap RO.
4. Break #4 is break between 8250 RO and 8230 RI on both the primary and the secondary path. The 8230 will wrap RI and the 8250 will wrap RO.

In all cases the 8230 and the 8250 also unwrap automatically if the cable is repaired.

The two remaining cases require a token-ring management module to automatically wrap the RI/RO ports of the 8250.

5. Break #5 is break between 8230 RO and 8250 RI on the secondary ring. The 8230 will wrap RO and the 8250 will wrap RI.
6. Break #6 is break between 8250 RO and 8230 RI on the primary ring. The 8230 will wrap RI and the 8250 will wrap RO.

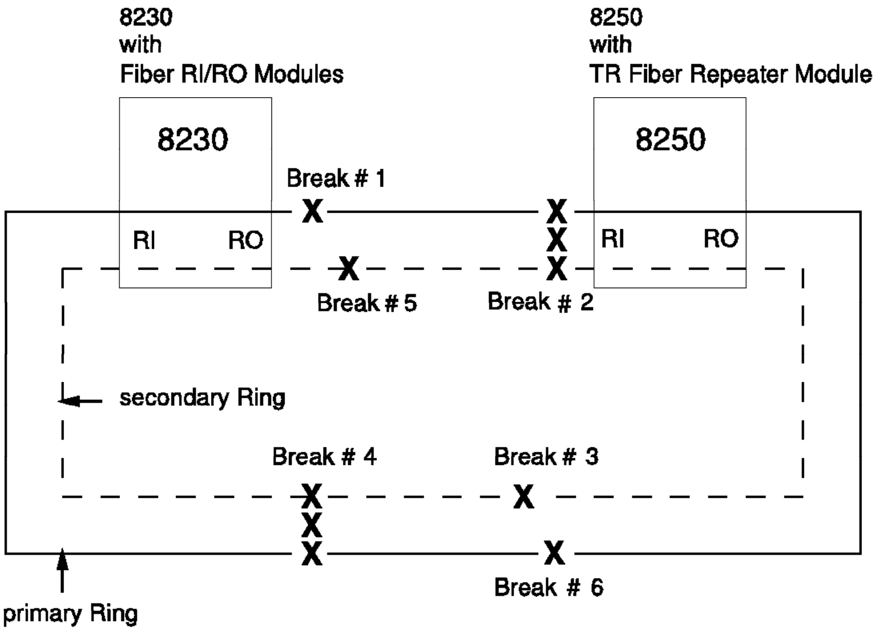


Figure 120. Break of 8230/8250 Connection

10.3.7 Configuring TR Fiber Repeater Module

To configure the token-ring repeater module, you must do the following:

- Enable/disable copper lobe ports

  This can be done via onboard dip switches or the following management module command:

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

  Each port can be enabled/disabled independently.

- Enable/disable fiber RI/RO ports

  This can be done via onboard dip switches or the following management module commands:

  ```
  SET TRUNK {slot} RING_IN.1 MODE {enable/disable}
  SET TRUNK {slot} RING_OUT.1 MODE {enable/disable}
  ```

The fiber RI/RO ports can be enabled/disabled independently.

- Enable/disable copper RI/RO ports

  This can be done via onboard dip switches or the following management module commands:

  ```
  SET TRUNK {slot} RING_IN.2 MODE {enable/disable}
  SET TRUNK {slot} RING_OUT.2 MODE {enable/disable}
  ```

  The copper RI/RO ports can be enabled/disabled independently from each other. This means that you may elect to use fiber cable for the RI while a copper cable is used for the RO, but be aware of possible problems in this type of configuration. See 10.3.4, "Network Segmentation" on page 228 for more information.

- Enable/disable copper RI/RO cable monitor mode

  This can be done via onboard dip switches or the following management module commands:

  ```
  SET TRUNK {slot} RING_IN {trunk} CABLE_MONITOR {enable/disable}
  SET TRUNK {slot} RING_OUT {trunk} CABLE_MONITOR {enable/disable}
  ```

  Note that you must use a special cable to connect two modules when using cable monitor mode.

- Set the token-ring speed to 4 or 16 Mbps

  This can be done via onboard dip switches or the following management module command:

  ```
  SET module {slot} RING_SPEED {4/16 mbps}
  ```

  As discussed before, the fiber repeater module can be connected to token-ring networks operating at 4 or 16 Mbps. You must set the correct speed before attempting to use the module.

- Assign the module to a backplane ring or set isolated (managed)

  This can be done using the following management module command:

  ```
  SET module {slot} NETWORK {network}
  ```

  In a managed environment, there can be up to a maximum of seven backplane token-rings. You can use the management module to assign the module to one of these rings or set the module to isolated mode. In an unmanaged environment, the position of the module within the 8250 will determine the network to which the module is assigned. The consideration for the unmanaged environment is the same as the 8250 token-ring media module.

- Enable/disable backplane interface (unmanaged)

  In an unmanaged environment, you can enable/disable the backplane interface via a dip switch. The backplane interface allows the fiber repeater module to establish connection with the other token-ring modules over the backplane.

  Note that when a new token-ring module is inserted into an unmanaged 8250, it will not be recognized by the other modules until a ring reconfiguration is performed. The ring reconfiguration is done using the LED check button.

- Set single/multiple rings mode (unmanaged)

In an unmanaged environment, dip switch setting on the token-ring fiber repeater module, and the token-ring media module, allows you to create one or multiple backplane rings.

If the modules are set to one backplane ring, all modules in the 8250 will operate on the same backplane ring. Thus the fiber repeater module can repeat and transmit data to any of the modules on the ring.

If you configure the modules for multiple rings, they will be assigned to one of the three (8250 Model 017) or two (8250 Model 006) networks on the backplane. In this case the slot in which the module resides determines the network to which the module is assigned. The slot/ring assignment in a multiple ring environment is given in 10.2.5, "Unmanaged 8250 Considerations" on page 219.

> **Note**
>
> In an unmanaged environment, all the token-ring modules within a single 8250 must be set to one ring or multiple rings. There may be unpredictable results if settings are not the same for all modules.

- Configure the module as an internal/external map source (managed)

  This can be done using the following management module command:

  ```
  SET TRUNK {slot} RING_IN {trunk} NETWORK_MAP {Internal/external}
  ```

  You must set the fiber repeater module to be internal or external network_map if you establish trunk connections using the copper RI and the special cables to take advantage of cable monitor mode. You do not need to set this mode if you have made your connection using the standard RJ-45 cable. This command, in part, determines what is displayed when you use the *show network map* command.

  Note that setting the internal/external map can only be done through a management module command.

- Enable/disable compatibility mode (8230)

  This can be done via onboard dip switches or the following management module commands:

  ```
  SET TRUNK {slot} RING_IN.1 COMPATIBILITY_MODE {enable/disable}
  SET TRUNK {slot} RING_OUT.1 COMPATIBILITY_MODE {enable/disable}
  ```

  Fiber trunk connection to an IBM 8230 needs the compatibility mode set to enable.

10.3.8 TR Fiber Repeater Configuration Example

Figure 121 on page 238 shows an example of using a token-ring fiber repeater module in conjunction with the 8-port token-ring MAU modules. In this example, two of these modules are used to connect two different 8250s each with a number of 8-port token-ring MAU modules.

Note in this configuration, the 8-port token-ring networks are connected to each other using the RI/RO ports provided on these modules, and the copper RI/RO ports on the fiber modules are used to connect the two 8250s. Note that this configuration is for illustration purposes; otherwise, there is no reason to use the fiber repeater module for this configuration, as an 8-port token-ring module could have performed the same function.

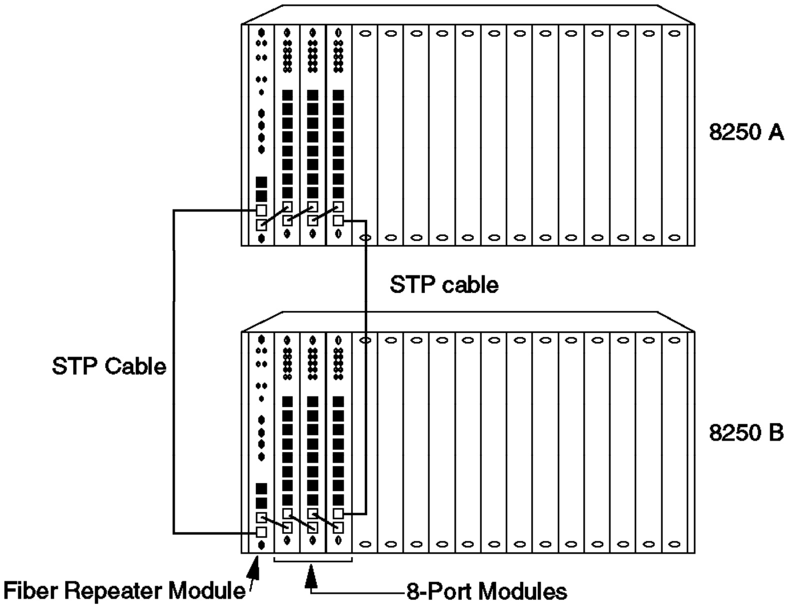


Figure 121. Configuration Example. TR fiber repeater module using STP cabling.

Figure 122 shows how the extended distances between 8250s can be achieved using token-ring fiber repeater modules.

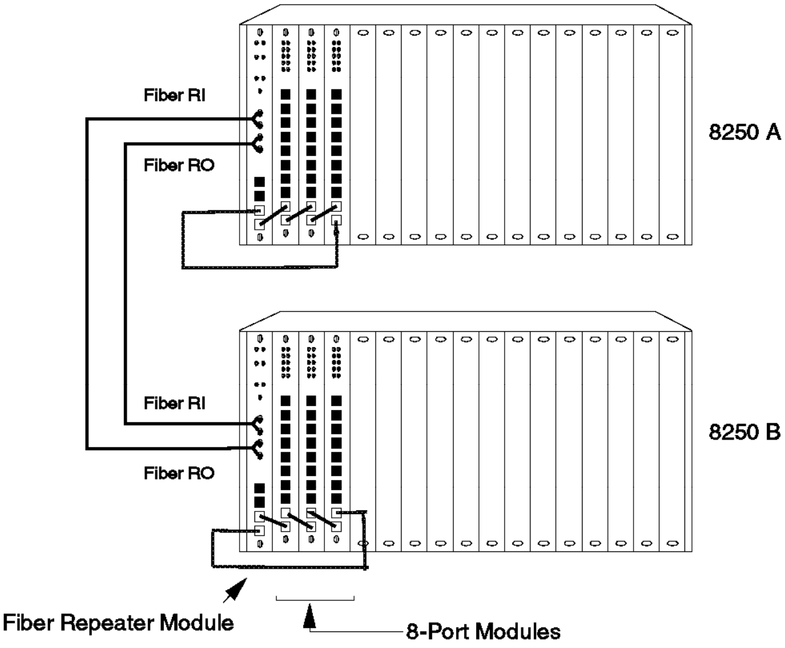


Figure 122. Configuration Example. TR fiber repeater module using fiber cabling.

Figure 123 on page 239 shows a configuration example where all three different types of token-ring media modules are used to form a single network extending over two buildings which are up to 2000 meters apart.

Note that the 8-port token-ring MAU modules are connected to each other and also to fiber repeater modules using external copper RI/RO cables. This is because the 8-port token-ring MAU modules do not provide a backplane interface. The connection between the fiber repeater modules and the 20-port token-ring module in 8250-B is over the backplane.

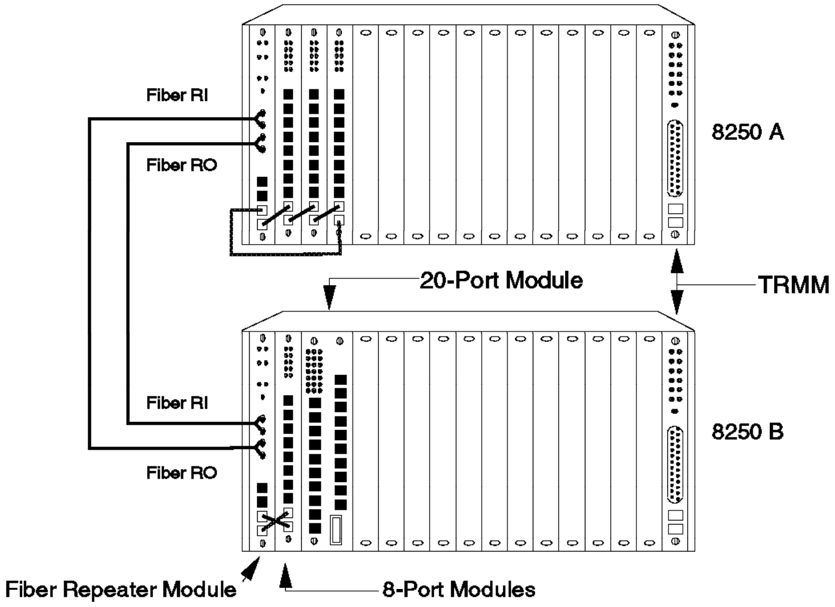


Figure 123. Configuration Example. Using all three different types of token-ring modules.

Figure 124 on page 240 shows an example of a *collapsed backbone*. In this example, there is a token-ring network on each floor of the building (Ring 1 and Ring 2 in this example). Rather than the traditional way of having the backbone network provided via a cable pulled through the risers in the building and connected to each of the *floor LANs*, we have connected each floor LAN to a central 8250 which is located somewhere in the building. This central 8250 will also provide the backbone ring (Ring 3) for connecting resources such as the mainframe, routers, and servers that normally are connected to a backbone LAN. The floor LANs can be connected to the backbone LAN via routers, bridges or bridge modules. In this example, we have shown the example of using external routers.

This configuration provides you with the ability to manage all the LANs and the interconnecting devices (such as the bridges) from a single point. For example, should the tracing of Ring 1 be required, the TAP stations can easily be plugged to the lobe port of the fiber module on the central 8250 that provides the connection to this LAN, allowing you to perform problem determination without having to move the TAP station where Ring 1 is located (as would be required in the case of a traditional backbone network).

Additionally, by locating an RS/6000 in the same location as the central 8250, you could also manage all the 8250s from the same location. Alternatively, you could use the *Telnet* facility offered by the TRMM to remotely log in to each floor 8250 and manage them remotely. However, note that EMMs do not support Telnet.

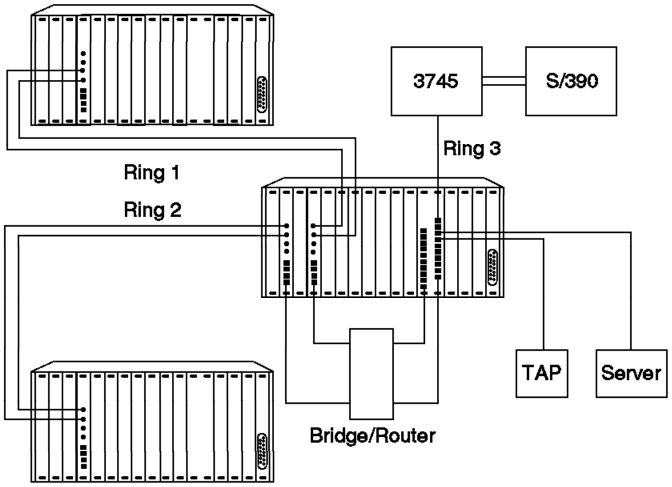


Figure 124. Configuration Example. Collapsed backbone.

10.4 Token-Ring Management Module

The 8250 token-ring management module (TRMM) is a network management module designed to work with the IBM 8250. TRMM provides connection to an IEEE 802.5 token-ring LAN enabling you to fully manage and control your token-ring network down to the port level. In addition, the TRMM contains advanced monitoring and control capabilities which allow you to configure and check status on all token-ring, Ethernet and FDDI modules in an 8250. The TRMM includes RI/RO ports for connection to other Multistation Access Units (MAUs).

The token-ring management module exists in different versions:

- Basic TRMM Version 1

  Announced in 9/92. Microcode can be updated to Basic TRMM Version 2 or the module can be upgraded to Advanced TRMM Version 2. The later upgrade consists of the new microcode and a daughter board, which has to be fitted on the TRMM.

- Basic TRMM Version 2

  Announced in 1/93. Can be upgraded to Advanced TRMM Version 2 as described above.

- Advanced TRMM Version 2

  Though a first version of this module did not exist, the module is named Version 2 because it is a superset of Basic TRMM Version 2. With Version 2 (basic or advanced) of the TRMM you can manage:

  - All 8250 Models (Model 6HC, 006 or 017)
  - All Ethernet modules, including the new 24-port 10BASE-T module
  - All token-ring modules, including the new token-ring bridge modules
  - All FDDI modules

The major features of the basic TRMM are as follows:

- The module complies with industry standards such as IEEE 802.5, TCP/IP, TELNET, SNMP and TFTP for integration into existing token-ring networks.
- Continuous monitoring and reporting of key network error statistics.
- Automatic detection and resolution of station beaconing with TRMM automatically closing the beaconing port to prevent disruption of the entire token-ring network.
- In-band/Out-of-band network management.
- Dynamic network control of the module to port level.
- Software assignable to one of seven separate token-ring networks on the backplane.

It is important to note that if a TRMM and an EMM are present in the same 8250, the TRMM must have higher *mastership* priority in order for beacon recovery to work. This is due to the fact that the current implementation of the EMM does not have the function to update any slave XMMs about configuration settings, and therefore the slave TRMM would not be aware of any other modules in the 8250 besides itself. A master TRMM does have the ability to update the other XMMs about configuration settings. This problem will be resolved with EMM Version 2.0, so that you can use either EMM or TRMM as the master management module without any loss of functionality.

If you have modules assigned to different token-ring networks in an 8250, you could use multiple TRMMs to track real-time statistics on the individual networks or have only one TRMM and assign it to the networks that you want the statistics for at any given time.

TRMM has a MAC instance including Ring Error Monitor (REM) function. The REM function does *not* have the ability to analyze the soft error MAC frames and thus places the ring in *soft error state*. Note that the token-ring MAC addresses for the 8250 have the format: **1000 F1XX XXXX**.

The TRMM offers a pair of non-repeated copper RI/RO ports. These RI/RO ports can be used for interconnecting token-ring MAU modules or external IBM 8228s or IBM 8230s via shielded twisted pair cables only.

These RI/RO ports support the cable monitor mode which is also provided with token-ring MAU and fiber repeater modules. When connecting the TRMM RI/RO ports to a non-8250 module, like the IBM 8228 or IBM 8230, *cable monitor* mode must be *disabled*.

cable monitor mode uses a DC-based signal on the RI/RO ports. If you did not *disable* this feature and attached the RI/RO ports to a non-8250 RI/RO port the 8250 RI/RO ports would wrap.

Note

TRMM does not support source route bridging. Therefore, you cannot perform tasks such as remote-login from one TRMM to another over a source route bridge or manage a TRMM via HMP/6000 over a source route bridge.

10.4.1 Front View and LED Description

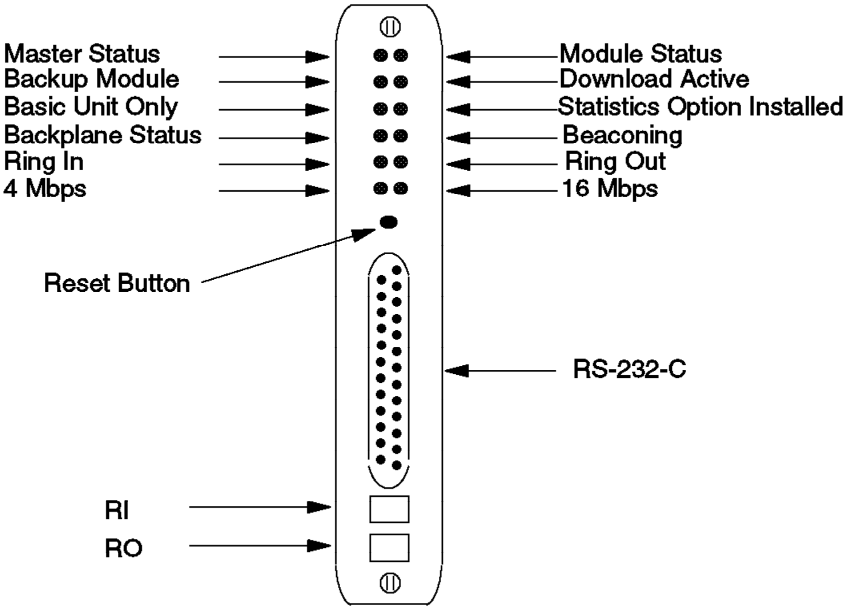


Figure 125. Front View of TRMM

Figure 125 shows the front view of the token-ring management module. Table 45 describes its various LEDs.

Table 45 (Page 1 of 2). TRMM LED Descriptions

LED name	Color	State	Description
Master module	Green	OFF	TRMM is slave.
		ON	TRMM is master.
Status	Green	OFF	Power off or complete failure.
		ON	Power on and software functioning properly.
Download	Yellow	OFF	Not downloading.
		ON	Download in progress.
Backup	Green	OFF	TRMM is master.
		ON	TRMM is slave.
Basic	Green	OFF	Advanced TRMM.
		ON	Basic TRMM.
Advanced	Green	OFF	Basic TRMM.
		ON	Advanced TRMM.

Table 45 (Page 2 of 2). TRMM LED Descriptions

LED name	Color	State	Description
Beaconing	Yellow	OFF	No beaconing.
		ON	Beaconing on the network.
Backplane	Green	OFF	TRMM is isolated.
		ON	TRMM is operating on the backplane.
RI/RO	Green	OFF	Port disabled.
		ON	Port enabled and functioning.
		1 Blink	Port is wrapped due to no cable detected.
		2 Blinks	Port is wrapped due to no signal detected.
4 Mbps	Green	OFF	Ring is operating at 16 Mbps.
		ON	Ring is operating at 4 Mbps.
		1 Blink	Ring is set to 4 Mbps but TRMM can not lock to signal.
16 Mbps	Green	OFF	Ring is operating at 4 Mbps.
		ON	Ring is operating at 16 Mbps.
		1 Blink	Ring is set to 16 Mbps but TRMM can not lock to signal.

10.4.2 TR Network Management Functions

The basic TRMM provides management and control capabilities in the following areas:

- Configurations

  When logged in under the administrator password, and the TRMM is the master management module, you can configure all the modules installed including the TRMM itself.

- Fault statistics monitoring

  You can set the TRMM to continuously monitor and report key error statistics by invoking the *monitor* command.

- Security control

  The TRMM provides two security features that prevent unauthorized access to devices on the network, address-to-port security and a 2-level password protection feature.

- In-band/out-of-band downloads

  The TRMM provides in-band download capability via FTP and out-of-band download via the RS-232 serial port on the TRMM.

- SNMP support

  The TRMM is an SNMP agent and can be managed via the AIX NetView Hub Management Program/6000.

- Remote login support

Using the *telnet* facility you are able to log in remotely to any TRMM and manage it from either a terminal attached to a remote TRMM or a workstation with TELNET support.

- Topology mapping

  The TRMM keeps a topological map of the TR modules in the 8250. The information in this map can be displayed via the *show network_map token_ring* command.

- Beacon recovery capability

  The TRMM senses a beaconing port and can resolve the beacon by disabling the faulty port, if necessary.

The Advanced TRMM provides all functions of the Basic TRMM and adds the following functions:

- Real-time performance monitoring

  Each advanced TRMM can serve as an independent real-time monitoring and control center for one token-ring network. It can continuously monitor and report such key statistics as network performance of the token-ring LAN and the stations attached to it. The ring performance is tracked through the collection of token rotation time statistics and ring usage. Station usage information is collected either in bytes or frames.

- Alarms

  The advanced TRMM allows the setting of thresholds which if exceeded, a network alarm is generated, to inform the network administrator of excessive network loads.

- Time of day security

  In addition to port access security that is provided on basic TRMM, the advanced TRMM provides an added level of protection called group-port security. This feature can be used to prevent access to the network for predefine d times and a given group of users.

When writing this book, we did not have access to the advanced TRMM module to fully explore these features.

10.4.3 Beacon Recovery Capability

When a station can no longer receive a signal from its Nearest Active Upstream Neighbor (NAUN), the station will initiate the beacon process. A beacon frame is sent by the station detecting the loss of signal and contains its own address as well as that of its NAUN. The beacon frame is sent to the local all-broadcast address (C000 FFFF FFFF).

The station that initiates the beacon process starts a timer. The purpose of the timer is to allow the NAUN to perform a self-test. When the NAUN receives the beacon frame with its address as the NAUN, it will remove itself from the ring and verify that it is able to receive and transmit frames by wrapping the receive and transmit pairs of the lobe cable. If the station is unable to receive or transmit frames, it will remain off the ring. If the station passes this self-test, it re-enters the ring.

In some situations, such as the station being configured at the wrong ring speed, the station is not able to receive the beacon MAC frame and it will therefore remain on the ring and the ring will continue to beacon. The downstream neighbor continues to send the beacon frame and the beacon recovery process cannot recover this type of error. The TRMM must intervene.

To maintain the integrity of the ring the TRMM allows enough time for the detecting station and its NAUN to remove themselves from the ring and verify that they are not the cause of the problem. If the ring is not repaired, then the TRMM can determine the faulty station and disable the port. Disabling the port isolates the lobe causing the problem.

Note

The TRMM can shut down a beaconing port only for modules that reside in the same 8250 *and* are on the same token-ring network as the TRMM. This means that you require one TRMM for each token-ring network per 8250 to cover your entire network.

To detect which station is causing the beaconing condition the TRMM builds a table of Port-to-MAC address translation by listening to the *active monitor present* and *standby monitor present* ring poll process. This is very similar to the way the IBM 8230 builds its table of MAC addresses-to-lobes translation. Since TRMM has a MAC instance and knows the order of physical ports within that 8250, it is able to determine which MAC addresses are attached to which ports *within* this 8250 and which MAC addresses are outside this 8250.

Note

The TRMM could also manage and perform beacon recovery for the 8-port MAU module which is located in this 8250 and is connected to the TRMM′s network.

For example, if a new station attempts to insert, with the wrong speed, into the token-ring network in that 8250, the TRMM knows about the new phantom voltage on that port; it also knows the beaconing station and its NAUN and their corresponding ports. It will, therefore, be able to determine that the new phantom voltage is between these two stations and will disable the beaconing port.

If the TRMM sees a beacon MAC frame from an address that is outside its 8250, it will automatically wrap any external RI/RO and therefore maintain the integrity of its part of the network. When the cause of the beacon has been resolved the user must *manually* enable RI/RO again, via the *set trunk ring_in/Ring_out mode* command. This is true for fiber RI/RO ports. In the case of copper RI/RO ports the situation is different. When the cause of the beacon has been resolved, the RI/RO ports are unwrapped and the ring is operational again without any manual intervention. TRMM takes advantage of squelch detection to do this.

If TRMM determines that the cause of the beacon is within its 8250 it will *not* wrap any external RI/RO.

10.4.4 Getting Started with a TRMM

Once the TRMM has been installed in the 8250 and a terminal is attached to the RS-232 port, the following should be done:

- Configure the terminal.
- Configure the TRMM.
- Configure the TRMM SNMP values (in-band only).

10.4.4.1 Configuring the RS232 Terminal

You must initially configure your terminal to the same parameter settings as the TRMM so the terminal and TRMM can communicate. You must match the TRMM factory defaults as shown in Table 46.

Note that the default settings for the TRMM and EMM are different. The EMM requires a setting of *2* for *stop_bits*, while the TRMM requires a setting of *1*.

Table 46. TRMM Terminal Parameter Options and Defaults

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

10.4.4.2 Configuring the TRMM

Once the terminal settings are done, you can configure the TRMM and all other 8250 modules. It is recommended that when using the TRMM for the first time you perform the following:

- Establish passwords.
- Set the internal clock.
- Configure other TRMM parameters.
- Set TRMM SNMP values.
- Set TRMM terminal for modem connection (optional).

Performing these tasks for TRMM is very similar to that of EMM which is described in detail in 7.11.2, "Getting Started with an EMM" on page 181. Please also refer to Chapter 15, "Token-Ring Management Functions" on page 343.

10.5 Token-Ring Bridge Module

The token-ring bridge modules are 2-port, 1-slot token-ring to token-ring bridges. One port is provided via the front panel in the form of a DB-9 connector for STP cabling and an RJ-45 connector for UTP cabling. The other port is selectable from among any of the seven internal token-ring segments on the backplane. Either port may operate at 4 or 16 Mbps.

There are two versions of the token-ring bridge module:

- **Token-ring SR bridge module**

The Source Routing (SR) bridge module implements a source route bridging protocol and is fully compatible with IBM Token-Ring bridges (IBM token-ring Bridge Program, IBM 8209 and the bridging function provided by the IBM 6611).

- **Token-ring SR/SRT bridge module**

  The SR/SRT bridge module implements both the Source Routing (SR) protocol and the Source Routing Transparent (SRT) bridging protocol. It can run in either mode as a user selectable option.

The modules use flash PROMs to save the configuration. An update of the bridge program can be done through a download of the new code from the RS-232 port provided on the bridge module′s front panel.

10.5.1 Front View and LED Description

Figure 126 shows the front view of the token-ring bridge module and Table 47 gives an interpretation of the various LEDs provided by the bridge modules.

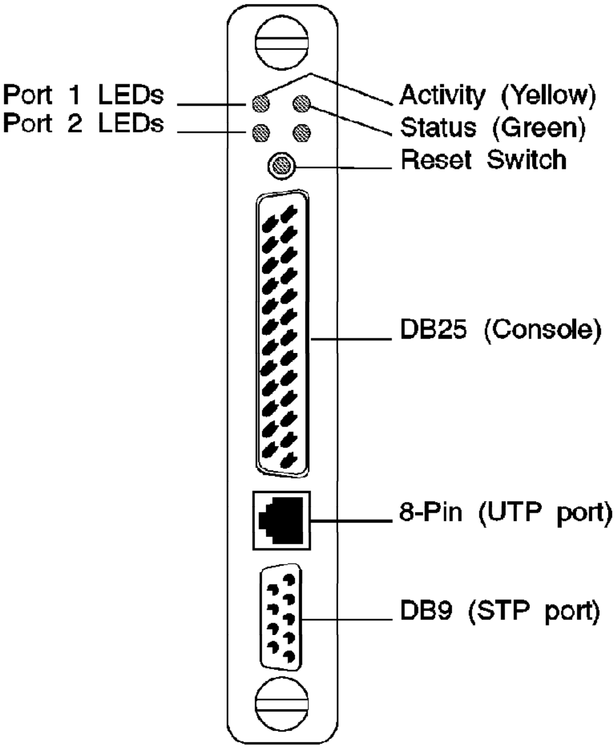


Figure 126. Front View of TR Bridge Module

Table 47 (Page 1 of 2). TR Bridge LED Descriptions

LED Name	State	Description
Status (green)	OFF	No power or port not inserted.
	ON	Port inserted and functioning properly.
	Blinking	Major module failure.

Table 47 (Page 2 of 2). TR Bridge LED Descriptions

LED Name	State	Description
Activity (yellow)	OFF	Port not passing traffic currently.
	Blinking	Port passing traffic intermittently.
	ON	Port passing traffic continuously.

10.5.2 TR Bridge Module and Network Management

The token-ring bridge module implements the following functions for network management:

- A front panel RS-232 port

  This RS-232 port can be used for the connection of an ASCII terminal as a management console. This terminal *must* be used for the initial configuration of the module. It provides configuration panels and gives error and performance statistics. The initial configuration can not be done from an SNMP manager.

- SNMP agent capability

  The agent conforms to TCP/IP and SNMP RFCs and provides a token-ring Management Information Base (MIB) compliant with RFC 1231.

- LAN Network Manager support

  The bridge module provides the following functions to support the IBM LAN Network Manager:

  - Configuration report server (CRS)
  - Ring error monitor (REM)
  - Ring parameter server (RPS)

The SNMP and the LNM management can coexist and run simultaneously.

To manage the bridge modules from a management module, a token-ring management module (TRMM) Version 2 is required (Basic or Advanced).

Note.

Current releases of EMM (V1.0 and V2.0) can not manage a token-ring bridge module.

10.5.3 Theory of Operation

The bridge consists of two token-ring interfaces, each connected to a link level processor and a large buffer for temporary storage of the incoming and outgoing token-ring frames. The buffer size is 512KB for each interface and there is an additional storage of 128KB for management control frames. A central microprocessor controls both token-ring ports and the buffer. The microprocessor and software logic decide which frames flow through the unit. See Figure 127 on page 249.

Transparent bridging logic decides to filter or forward a frame based on address filtering tables that are continually updated by the hardware.

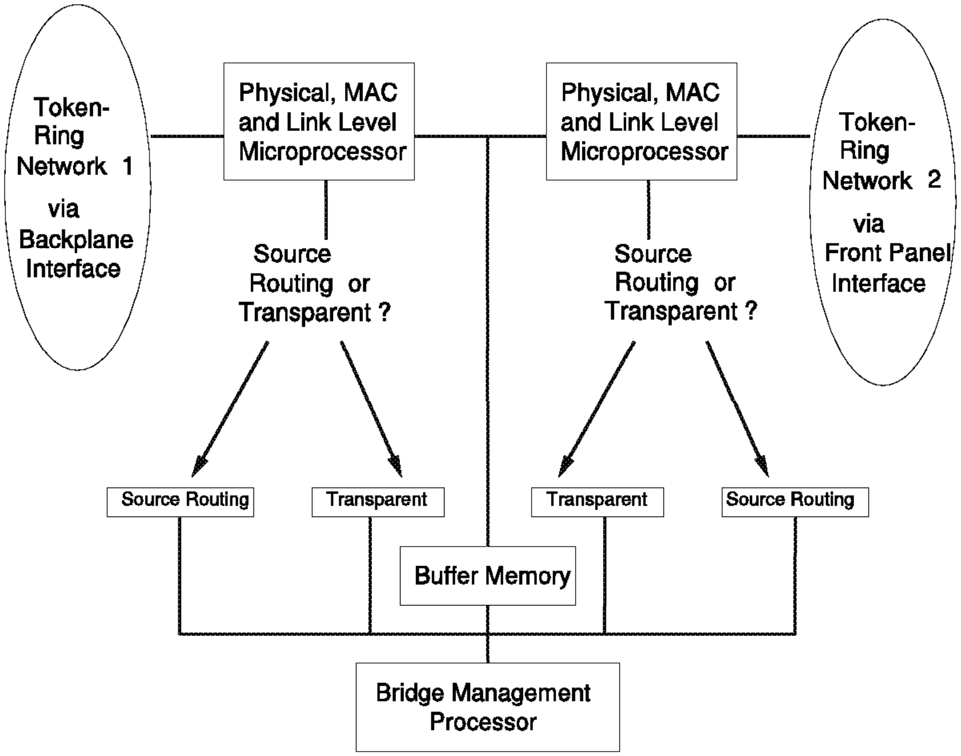

Token-Ring Network 1 via Backplane Interface
Physical, MAC and Link Level Microprocessor
Physical, MAC and Link Level Microprocessor
Token-Ring Network 2 via Front Panel Interface
Source Routing or Transparent ?
Source Routing or Transparent ?
Source Routing
Transparent
Transparent
Source Routing
Buffer Memory
Bridge Management Processor

Figure 127. TR Bridge Block Diagram

10.5.4 Installation and Operation of the Bridge Modules

After insertion of the module into the concentrator, the module performs a series of internal self-tests. The tests take approximately 15 seconds and include processor checks, firmware integrity tests, memory tests and interface controller tests.

The bridge module can be connected to other modules and devices in a variety of ways, depending on the requirements of the network. Use the following general guidelines when establishing physical connections from the token-ring bridge module to other devices:

- Ring 1 attaches to the 8250 backplane via a connector on the backend of the module.
- Ring 2 has two connectors, an RJ-45 and a DB-9, used to connect to either UTP or STP media, respectively. It can be configured for either media; however, only one media may be active at a time.
- The selected front panel connector can be attached to a lobe port on another 8250 token-ring module, or to an external Multistation Access Unit (MAU).

10.5.4.1 Configuring the TR Bridge Module

Once the module has been installed in the concentrator, you must perform the initial configuration. For this initial configuration an ASCII terminal must be attached to the front panel RS-232 port of the module. After completion of the bridge tests, a main menu is displayed on the terminal. From the main menu you can select any of the following:

- **Basic Configuration Menu**, from which you set basic parameters that establish the bridge as a station on your network.
- **Detailed Configuration Menu,** from which you configure the bridge to operate in your environment.
- **Statistic Reporting Menu,** which provides reports about the bridge (throughput, hop counts, errors).
- **Utility Menu,** which provides additional special case configuration options, as well as a utility to download software upgrades.

The **Basic Configuration Menu** provides the following parameters:

- Ring number for port 1 and port 2.

  In a source routing environment, each ring must be identified by a unique number between 1 and X′FFF′. The ring on port 1 is the one connected to the backplane, whereas the ring on port 2 is connected to the front panel.

- Bridge number (a value from 0 to X′F′)

The **Detailed Configuration Menu** provides the following options:

1. **Port configuration**

   - Port state

     In a manual configuration (that means the spanning tree is turned off) you can specify the port state to be the following: disabled, blocked, listening, learning or forwarding.

   - Spanning tree explorer frame forwarding

     In a manual configuration, the forwarding of explorer frames can be turned *on* or turned *off* on a per port base.

   - Hop count limit (1-7)

     The maximum number of routing descriptors allowed in all-route explorer (all-route broadcast) or spanning tree explorer (single-route broadcast) frames.

   - Early token release mode

     Only valid for 16 Mbps rings.

   - Port path cost

     Used by the spanning tree algorithm to select the minimum-cost path toward the spanning tree root bridge.

   - Port priority

     Used by the spanning tree algorithm to resolve routes with equal path costs.

   - Maximum address age

     Address table entries in the forwarding database are discarded after this time value (applicable for SRT bridges only).

   - Local MAC address (locally administered address)

     If you do not define a locally administered address, the burnt-in address of the bridge adapter is used.

   - Ring speed (4/16 Mbps)

     This value does not have to be the same for both ports.

2. **Bridge configuration**

   - Bridge IP address for SNMP management
   - Default SNMP manager address

     This is the address that the bridge module will send SNMP traps to.

   - UDP checksum mode

     Turns UDP checksum on or off and must match the setting in the SNMP manager.

   - SNMP configuration (community name, system location, system name, system contact)

3. **Spanning tree configuration**

   The spanning tree algorithm requires certain parameter settings. The bridge module comes with preset default values which should be acceptable in most cases.

   - Port path cost

     The port path cost defines the relative cost of using this port as a path to the root bridge. The costs are generally a function of the speed of the LAN.

   - Port priority

     This defines the priority of the port in relation to other ports within the bridge.

   - Maximum age

     This is the time in seconds, any port within the spanning tree network will wait before timing out its protocol information.

   - Hello time

     This is the time in seconds at which the root bridge will generate *hello* frames, which are used to propagate protocol information to all participating bridges.

   - Forwarding delay

     The time a bridge port spends in the listening and learning state.

   - Bridge priority

     The bridge priority defines the priority field of the bridge identifier.

   - Bridge type (SR, SRT)

     Sets the bridge software for either source routing (SR) or source routing transparent (SRT) mode. This applies only to the SR/SRT bridge module.

   - SR forwarding ON/OFF

     When set to off, the bridge will not forward any source routing frames.

10.5.4.2 Entering a Backplane Ring

After the installation, power-up, and initial configuration of the module are complete, you must insert the module′s backplane port into a backplane ring.

If you are using the module in an unmanaged hub, a jumper on the module must be set. This jumper selects the assignment of the backplane port to operate in single ring or multiple ring mode as described for the token-ring media module.

Then the backplane must be re-initialized to include this module in the ring, by pressing the *reset button* three times.

If you have a network management module in the concentrator, add the bridge to a backplane network using the following management command:

```
SET module {slot} NETWORK {isolated or token_ring_n}
```

There are two other settings that can be configured with a network management module. The front panel active port selection is done with the following command:

```
SET PORT {slot.2} ACTIVE_CONNECTOR {DB9 or RJ-45}
```

The following command can be used to select the ring speed:

```
SET PORT {slot.port} RING_SPEED {4mbps or 16mbps}
```

10.5.4.3 TR Bridge Statistics

The token-ring bridge module provides the following statistical information:

1. **General Statistics** which provide the following traffic statistics for each port:

   Forwarded frames
   Multicast frames forwarded
   Single route explorer frames
   All routes broadcasts
   Local frames forwarded
   Local frames received
   Security filtered frames
   Maximum hop filtered frames
   Forwarding rate (current and peak)
   Throughput (current and peak)

2. **Histogram Statistics** which display the following:

   Number of frames for each hop count (1-7)
   Frame size distribution

3. **Error Statistics** which list the following error counts for each port:

   Line errors
   Burst errors
   ARI/FCI errors
   Lost frames
   Congestion errors
   Frame copy errors
   Token errors
   Signal losses
   Hard errors
   Soft errors
   Xmit beacon count
   Wire faults
   Auto removals
   Remove received
   Single stations detected
   Ring recoveries

10.5.4.4 TR Bridge Utilities

The bridge module′s utilities provide you with the following:

- Filtering address table display

  Displays the filtering MAC addresses which are learned by the transparent bridging logic of the bridge.

- Error logger mode

  Allows you to set the bridge module to stop operating or to restart in case of an error.

- Display/clear error log

  Allows you to display or clear the error messages recorded by the bridge module.

- Initiate the flash loader

  Allows you to perform out-of-band software upgrade.

10.5.4.5 TR Bridge Filtering

In general, filters provide selective blocking of frames that otherwise would be forwarded by the bridge. The bridge module allows the filtering of frames based on Destination Service Access Point (DSAP) and on Sub-Network Access Protocol (SNAP).

Frames on token-ring LANs follow the IEEE 802.2 Logical Link Control (LLC) standard. LLC allows multiple applications to operate in a single station. The LLC header contains source and destination service access points (DSAP and SSAP) which are used to determine the respective applications. Table 48 shows some common SAPs:

Table 48. Common SAPs

SAP Value	Address Type
FF	Global SAP
FE	OSI Network Layer
F0	IBM NetBIOS
E0	Novell Netware
B0	3COM Protocol
04	IBM SNA
AA	TCP/IP SNAP Protocol

The Sub-Network Access Protocol (SNAP) is an extension of the LLC format. It uses a predefined LLC consisting of a DSAP and SSAP of X′AA′ and an additional *type* field. The type field value is defined for many applications. For example, the Internet Protocol (IP) uses the value X′0800′, while the Address Resolution Protocol (ARP) uses X′0806′.

To activate a DSAP or SNAP filter, the *special filtering enable switch* for the given port must be set to ON and the corresponding DSAP or SNAP values have to be defined.

Note that the current release of the TR bridge module has no MAC address filtering implemented.

10.5.5 Load-Sharing Backbone

The token-ring bridge module can be used to build a redundant and load-sharing backbone network. Figure 128 shows an example of such a network with three 8250 hubs. Each hub contains a TR management module, two TR fiber repeater modules, two TR bridge modules and a maximum of five 20-port TR media modules.

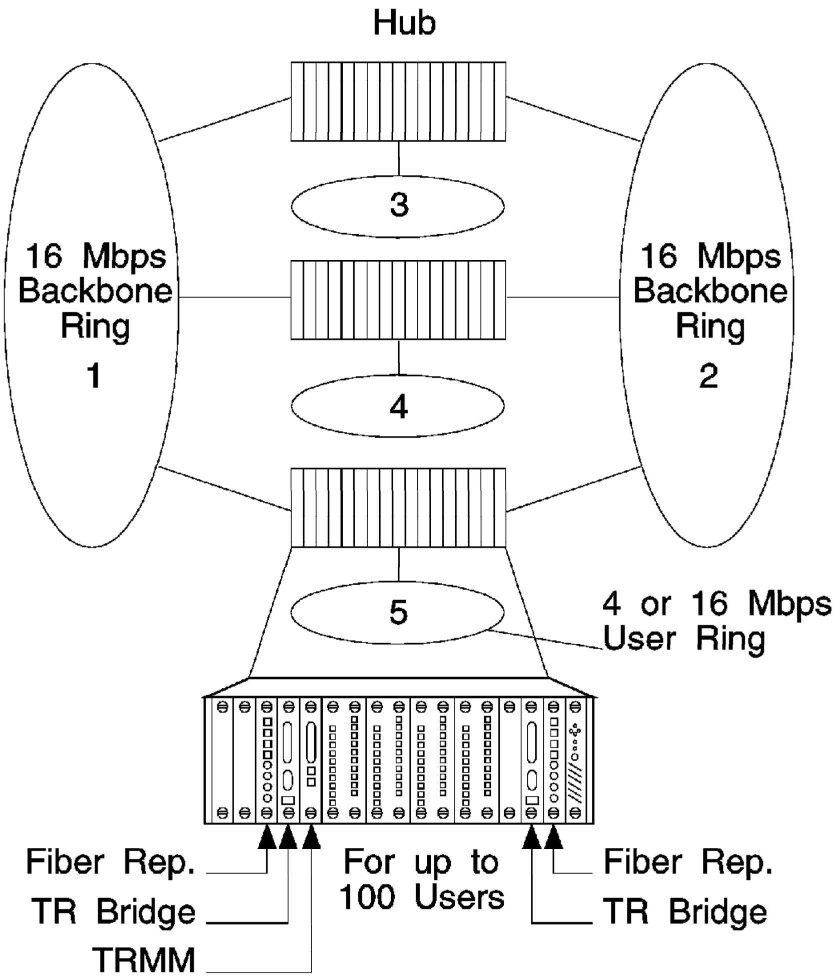


Figure 128. Load-Sharing Backbone

10.6 Token-Ring Accessories

Some accessories are needed to have a complete installation. For the token-ring network these accessories are:

- Shielded twisted pair patch cable

  When the 8250 is used with the IBM cabling system to build token-ring networks a twisted pair patch cable with an RJ-45 connector at one end and a universal data connector at the other end is needed. This cable connects the 8250 ports with their shielded RJ-45 connector to the patch panel with the IBM Data Connector. Two patch cables are proposed for that purpose, one with an overall length of 4 feet (1.27 m) and the other with a length of 8 feet (2.49 m).

- STP cable for RI/RO ports

  The purpose of this cable to connect the RI/RO ports of token-ring modules when cable monitor mode is enabled. This allows the modules to sense a cable fault, and automatically wraps the ring to keep it up and running. The STP cable for RI/RO is available in two different lengths (10 inches or 30 inches). One 10-inch cable comes with each TR MAU module. The 30-inch cable can be ordered separately.

- Token-ring UTP media filter

  The token-ring UTP media filter links a network station to 4 or 16 Mbps token-ring networks which are using unshielded twisted pair (UTP) cabling. The filter provides the following functions:

  – It converts the connector on a token-ring adapter card from DB-9 to 8-pin modular connector.
  – It matches the impedance from 150 ohms to 100 ohms.
  – It reduces the the radio frequency emissions for FCC class A compliance.

For more details about these accessories, refer to the *IBM 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide*(GA33-0191).

Chapter 11. 8250 FDDI Modules

This chapter contains the description and configuration information about the following modules:

- FDDI Fiber Module
- FDDI STP Module
- FDDI Management Module

11.1 FDDI Fiber and FDDI STP Module

The FDDI media modules (fiber or STP) are 2-slot modules which provide eight ports for connecting Single Attachment Stations (SAS) to an FDDI backbone. Two of these ports (ports 1 and 2) can be either Master (M) or Slave (S) ports, offering the flexibility to use the FDDI media module as:

1. A stand-alone concentrator
2. As part of a tree of concentrators
3. In a redundant slave configuration

The other six ports (ports 3 through 8) are always M ports. See 2.8.2, “Port Types” on page 37 for a description of the different FDDI port types.

You can install up to a maximum of four FDDI fiber/STP media modules in an 8250 Model 017, allowing you to set up an FDDI network with a maximum of 32 stations attached to a single 8250. The 8250 Model 006/6HC allows the installation of two FDDI fiber/STP media modules.

The FDDI media modules comply with the ANSI FDDI standards to provide interoperability with other products, such as the IBM 8240, which implement this standard. The fiber version uses ST type connectors for 50 or 62.5 micron fiber, and the STP version uses DB-9 connectors for shielded twisted pair.

These modules provide *Dual Homing* via connection to an FDDI Dual Access Station (DAS) for added redundancy and reliability.

The ability to configure redundant S ports on these modules allows you to set up redundancy with cascading concentrators in a dual ring tree configuration.

The FDDI media modules do not incorporate dip switches. A management module is required to be installed on the 8250 before FDDI modules can be used in an 8250.

Examples of undesired configurations using the 8250 FDDI modules are provided in the *IBM 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide* (GA33-0191).

11.1.1 Front View and LED Description

Figure 129 and Figure 130 show the front view of the FDDI fiber and STP media modules respectively.

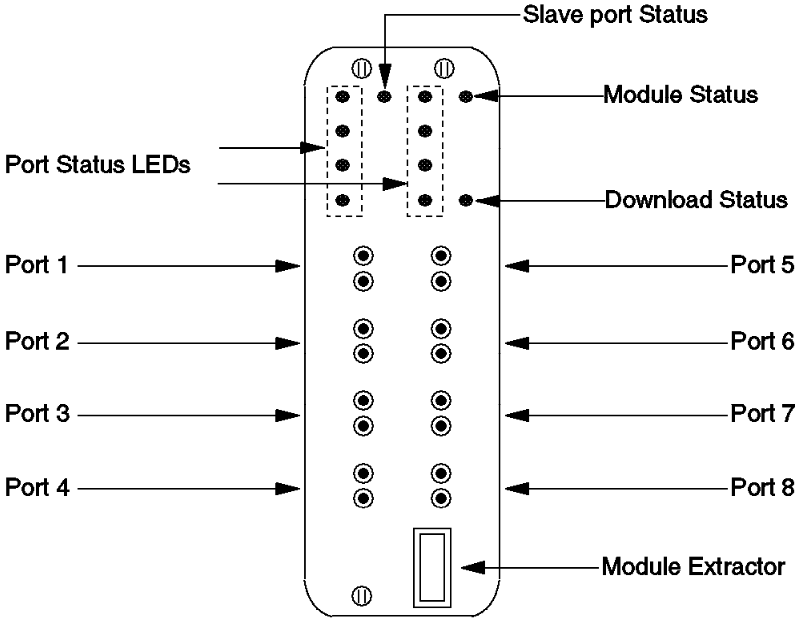


Figure 129. FDDI Fiber Module Front View

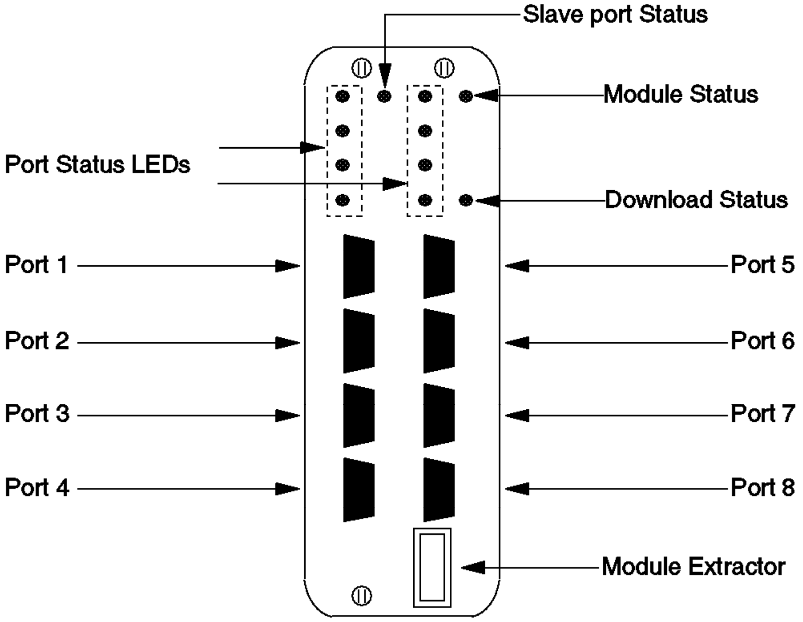


Figure 130. FDDI STP Module Front View

The FDDI media modules (fiber or STP) have 11 LEDs on the front panel that indicate the status of each port and of the module. Table 49 on page 259 describes the meanings of these indicators.

Table 49. FDDI Media Module LED Description

LED Name	Color	State	Description
Port Status	Green	OFF	Port disabled.
		ON	Port enabled and active.
		1 Blink	Port enabled but not active.
		2 Blinks	Illegal configuration or link failure.
Slave Port	Green	OFF	No selected slave port.
		ON	Port 1 configured as slave port.
		1 Blink	Port 2 configured as slave port.
		2 Blinks	Ports 1 and 2 both enabled as slave ports.
Module status	Green	OFF	Module is not receiving power.
		ON	Module is powered up and operating.
Module status	Yellow	ON	Module is being downloaded.

11.1.2 Configuration Guidelines

The following guidelines, as defined by the FDDI standard, should be followed when designing your FDDI network:

- The total length of the network fiber must not exceed 200 km. This distance must include the length of the secondary ring, if a dual ring is implemented.
  - The maximum distance between wiring concentrators must not exceed 2 km.
  - The distance between wiring concentrators and attached stations must not exceed 2 km for fiber and 100 m for STP. For more information about the cable specifications and distance limitations, refer to *IBM 8250 Multiprotocol Intelligent Hub Planning and Site Preparation Guide (GA33-0191)*.
- The maximum number of stations is limited to 500.
- The maximum number of wiring concentrators in an FDDI network is limited by the maximum number of stations that can connect to the ring.
- The maximum number of wiring concentrator sublevels in a tree structure is limited by the maximum number of stations that can connect to the ring.
- The optical attenuation between ports on a wiring concentrator or between concentrators and stations should not exceed 11 dB for 62.5/125 micron cable, and 7.0 dB for 50/125 micron cable.
- All port connections must follow the rules defined in Table 50.

Table 50 (Page 1 of 2). Connection Rules for Single and Dual Attachment Stations

Station Port Type	Fiber Module Port Type	Rule
A	M	Tree connection with possible redundancy. Port B shall have precedence for connecting to a Port M in a single MAC node.
A	S	Undesirable peer connection that creates a wrapped ring.

Table 50 (Page 2 of 2). Connection Rules for Single and Dual Attachment Stations

Station Port Type	Fiber Module Port Type	Rule
B	M	Tree connection with possible redundancy. Port B shall have precedence for connecting to a Port M in a single MAC node.
B	S	Undesirable peer connection that creates a wrapped ring.
M	M	Invalid configuration.
M	S	Normal tree connection.
S	S	Connection that creates a single ring of two slave stations.
S	M	Normal tree connection.

Note that the A and B ports identified in this table are not available on the FDDI fiber or STP media modules. However, the FDDI management module does provide A and B ports.

11.1.3 Configuring the FDDI Fiber and STP Modules

To be able to use the FDDI media modules (fiber or STP) you have to configure them. This can only be done via a management module installed on the 8250.

The following steps are required to configure an FDDI media module:

- Assign the module to a backplane ring or set isolated

  When you first install the module, it will default to isolated mode. The following command can be used to change the network assignment for the module:

  ```
  SET MODULE {slot} Network {fddi_n or Isolated}
  ```

- Set the port type

  When you first install the module, all ports default to M (Master) type. If necessary, you can change the type of port 1 and/or 2 to S (slave). The following command can be used to do this:

  ```
  SET PORT {slot.port} TYPE {master or slave}
  ```

- Enable/disable ports

  When you first install the module, all the ports are disabled. You can enable/disable ports, individually, using the following command:

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

- Save module configuration

  After configuring the FDDI media module, you should issue the following command to save the current configuration in the management module′s non-volatile memory:

  ```
  SAVE MODULE_PORT
  ```

  This command saves the current configuration of all the modules and ports in the management module′s memory. If the FDDI media module is removed and then inserted after issuing the above command, the configuration will be based on the information currently saved in the management module.

Note that the FDDI media modules are two-slot modules. All the commands issued for these modules should refer to the right-most slot number. This slot number is also used by the modules themselves to report to the management module.

11.1.4 FDDI Topologies Using Media Modules

11.1.4.1 Stand-alone Workgroups

Figure 131 shows an example of using an FDDI fiber Module to set up stand-alone workgroups in a single 8250. In this example, each FDDI fiber module is set to isolated, allowing the stations attached to each module to communicate only with each other, resulting in two distinct FDDI networks.

Since the maximum number of FDDI fiber modules which can be installed in a single 8250 Model 017 is four (because of power requirements), you can have up to a maximum of four FDDI networks in this type of configuration.

Note that these modules are isolated and are not using the backplane for passing data between the stations.

In this configuration, all ports must be configured as M ports.

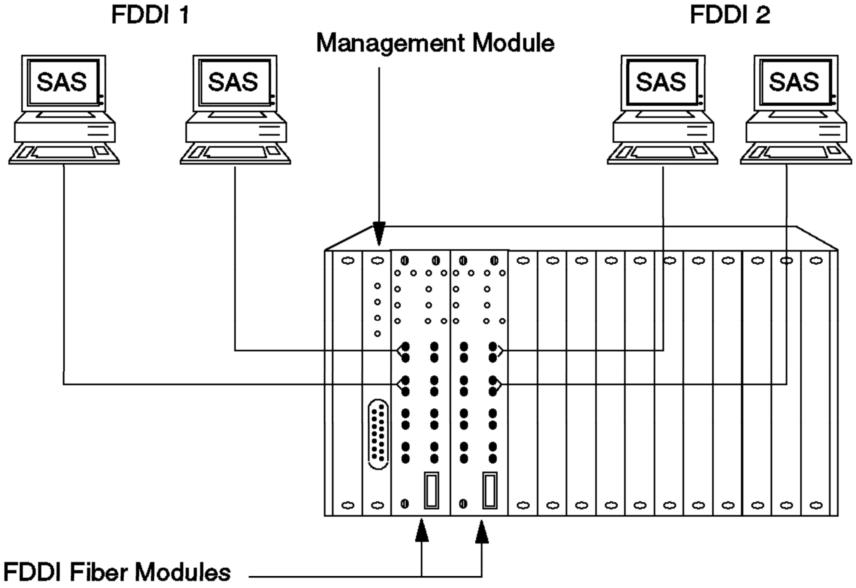


Figure 131. Fiber Stand-Alone Workgroups

11.1.4.2 Stand-Alone Concentrator

In Figure 132 on page 262, all the FDDI fiber modules are assigned to the same FDDI network on the backplane, allowing you to set up an FDDI network with a maximum of up to 32 stations. In this configuration, all the ports must be configured as M ports.

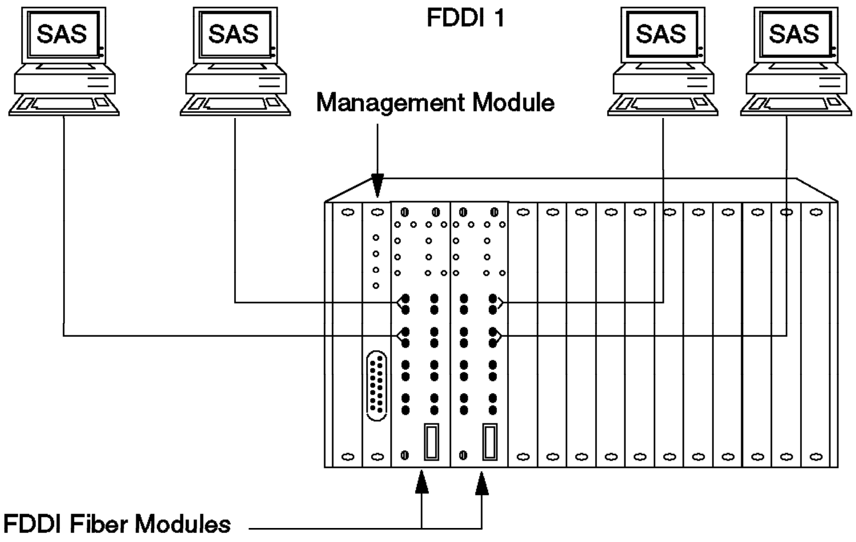


Figure 132. Fiber Stand-Alone Concentrator

11.1.4.3 Stand-Alone Concentrator with DAS

Figure 133 on page 263 is the same as the previous example plus the additional dual access station.

In this case, a *server* is connected (via its A and B ports) to two M ports on the FDDI fiber module. The main data path will be between the B port and its corresponding M port on the FDDI fiber module. The path between the A port on the station and the corresponding M port on the FDDI fiber module will be in backup mode. Should the main path fail (due to a link or fiber module failure), the backup path will be activated automatically to allow the server access to the FDDI network.

Although both ports on the DAS could have been connected to the same FDDI fiber module, for the sake of added redundancy (in case of module failure), in this example we have connected the workstation to two different fiber modules.

Note that both fiber modules are attached to the same backplane FDDI network.

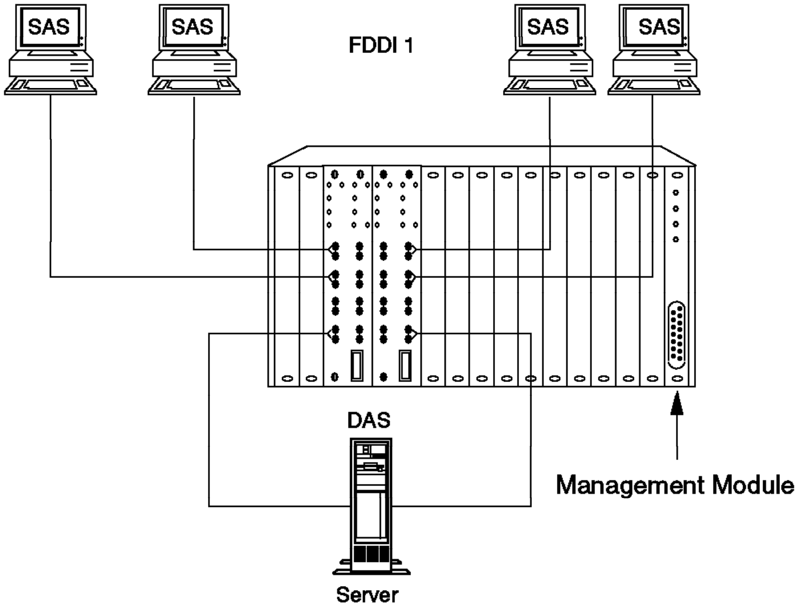


Figure 133. Fiber Stand-Alone Concentrator with DAS

11.1.4.4 Tree Topology

In Figure 134 on page 264 we have set up a tree topology consisting of two 8250s. In this case, each 8250 can have up to a maximum of four FDDI fiber modules.

As can be seen, in this configuration, the tier-2 8250 uses the S port to connect to the M port in the tier-1 8250.

This kind of topology will address the requirements of organizations that need to interconnect large numbers of users by allowing multiple 8250s to be connected to each other in a hierarchical manner.

Also note that, in this example, we have connected a DAS (server) to both 8250s, to provide redundancy in case of an 8250 failure.

In this type of configuration, you could have more than the two levels of concentrators which is shown in this example. For instance, a third concentrator could have been connected via its S port to the M port on the tier-2 8250.

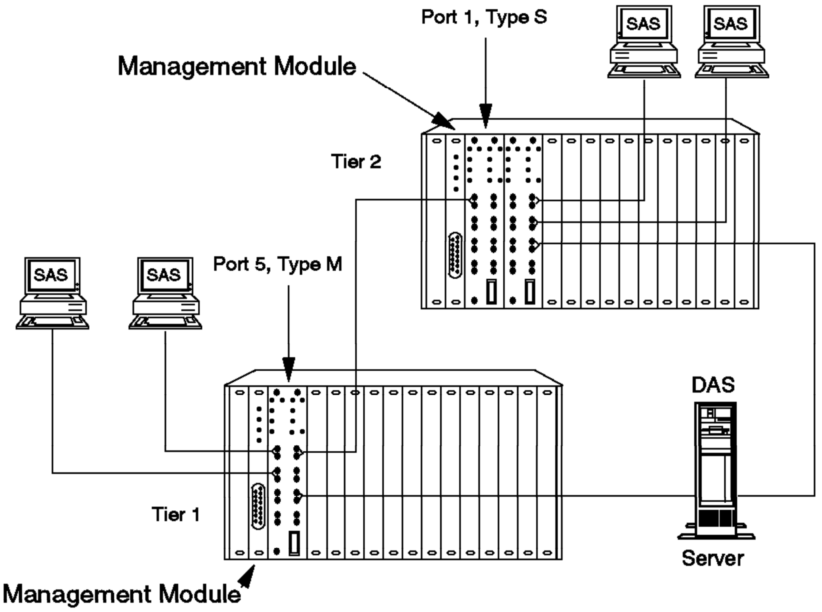


Figure 134. Tree Topology

11.1.4.5 Tree Topology with Link Redundancy

To provide link redundancy for a tree topology, we can use a second link to connect the S port on the tier-2 8250 to the M port on the tier-1 8250. This would allow the backup link to automatically take over should the primary link fail. This is shown in Figure 135 on page 265.

In this case we have to use the following command to enable redundancy between the two ports on the fiber modules:

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

Note

Redundant slave connections can be made to modules on the same network, but the ports do not have to be on the same module.

Note that in any redundant link configuration, only one end of the link should be designated as a redundant link. This means that the above command should be entered only in one of the two 8250s.

In redundant link configuration, the active port passes data while the backup link does not pass any data in either direction until the primary link fails.

If you want to provide redundancy as shown in this configuration, you must ensure that both S ports are on the same 8250, and both M ports are on the other 8250. If you mix the M and S ports, you will have a dual ring configuration.

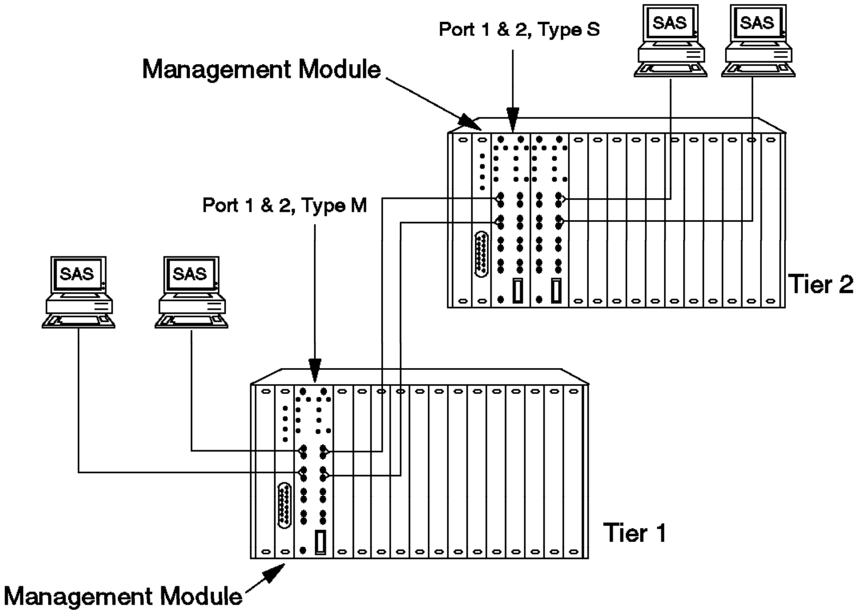


Figure 135. Tree Topology with Link Redundancy

11.1.4.6 Redundant Slave Ports

The configuration in Figure 136 on page 266 shows how an 8250 with the FDDI fiber modules can be connected to the FDDI dual ring using a dual access concentrator (such as an IBM 8240).

This configuration allows the backup port to automatically take over should the primary link fail.

As mentioned in the previous example, you must use the *set port mode* command to enable redundancy between the two ports on the 8250 FDDI fiber module and note that while the primary port is operating normally, the backup port does not pass any data.

In this example, note that the primary and backup port are on different 8250 FDDI fiber modules. However, this does not have to be the case.

In this configuration, we have shown an 8240 as a means of connection to the FDDI dual ring. However, the use of an 8240 is not necessary if an FDDI management module is installed in the 8250. In that case, you can use the A and B ports provided on the FDDI management module for connecting the 8250 directly to the FDDI dual ring. The FDDI management module is discussed in 11.2, “FDDI Management Module” on page 267.

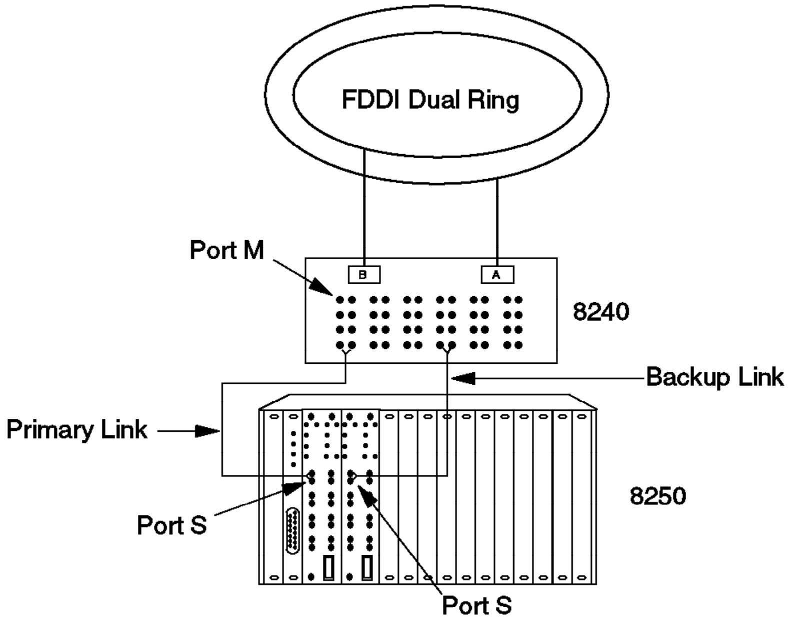


Figure 136. Redundant Slave Ports

11.1.4.7 Dual Homing

Figure 137 on page 267 shows how you can achieve dual homing by using the the redundant feature offered on the S port of the 8250 FDDI fiber/STP modules.

As can be seen, the FDDI fiber modules are connected via their S ports to the M ports on two different 8240s which have in turn been connected to the FDDI dual ring via their A and B ports. By using the *set port mode* command we can make one of the S ports on the 8250 act as the redundant port for the other S port. This allows the backup port to take over automatically if the primary port fails.

This configuration provides an alternate path to the FDDI dual ring in the case of 8240, link or FDDI fiber module failures.

If an FDDI management module is installed in the 8250, you could use the A and B port provided by the management module to set up a similar configuration.

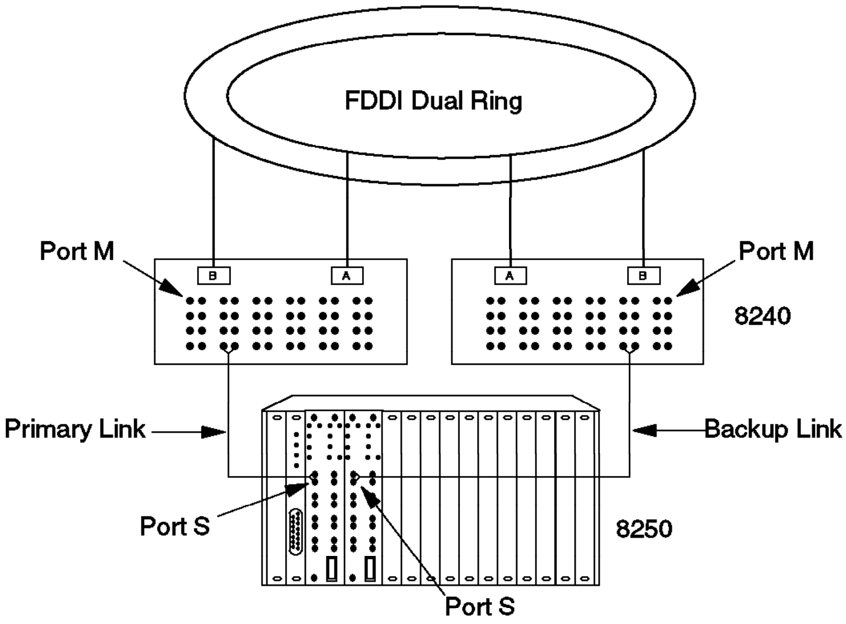


Figure 137. Dual Homing

11.2 FDDI Management Module

The FDDI management module is a 2-slot module with an FDDI Medium Access Control (MAC) address. It provides A and B ports for uplink connections to another 8250, or an IBM 8240 FDDI wiring concentrator. A connector to an optical bypass switch is also provided.

The FDDI management module supports FDDI Station Management (SMT) 6.2. It can also serve as an independent real-time monitoring and control center for an FDDI ring, by collecting and reporting key statistics (MAC counters), network events, and neighbor information.

11.2.1 Network Management Functions

The FDDI Management Module (FMM) provides the following management and control capabilities:

- Configurations

  If configured as the master management module, the FMM will allow you to configure an 8250 and all its modules. The configuration function is similar to that of TRMM and EMM.

- Fault Statistics Monitoring

  FMM will allow you to monitor and report key statistics about the FDDI network to which it is attached. These statistics are updated periodically, providing a snapshot of the network at any given time.

- Security Control

  The FMM provides a two-level password protection feature to prevent unauthorized access to the management module. The *security control* function is similar to that of TRMM and EMM.

- Out-of-Band Downloads

  The FMM provides out-of-band download features which allows to upgrade the firmware of the FMM via a connection to the RS-232 serial port on the front panel of the FMM.

- SNMP Support

  The FMM acts as an agent in an SNMP-managed environment, responding to SNMP requests and generating SNMP traps. This is similar to the functions provided by TRMM and EMM.

- Telnet Support

  The FMM supports remote login from any device on the network which supports Telnet, allowing management from a terminal attached to a remote FMM/TRMM or a workstation with Telnet support. This function is similar to that of TRMM.

- Mapping

  The FMM provides a mapping feature that keeps a detailed topological map of the 8250 concentrator and its FDDI modules.

- Fault Detection and Recovery

  The monitor and control capability of the FMM is protocol independent, thereby, enabling you to use it as the master management module in the 8250 with Ethernet, token-ring, and FDDI modules.

11.2.2 Front View and LED Description

The front panel of the FDDI management module consists of the following components, as shown in Figure 138 on page 269:

- Six LEDs for the monitoring of the module status.
- One button to reset the module
  - This button should be used only when you suspect problems with the FMM. This action requires the tip of a small device, such as a pen or a small screwdriver. This is because the button is recessed to prevent an accidental reset.
- One RS-232 serial port connector used to connect the FMM to a terminal or modem.
  - The 25-pin (DB-25) RS-232 serial port is a male connector used to connect the FMM directly to a terminal or modem. Such connections allow you to enter management commands locally, and also allow you to download new software into the FMM.
- One optical bypass connector for connection to an optical bypass switch.
- Two Media Interface Connectors (MIC) for connection to other FDDI devices. The MICs function as the A and B ports.

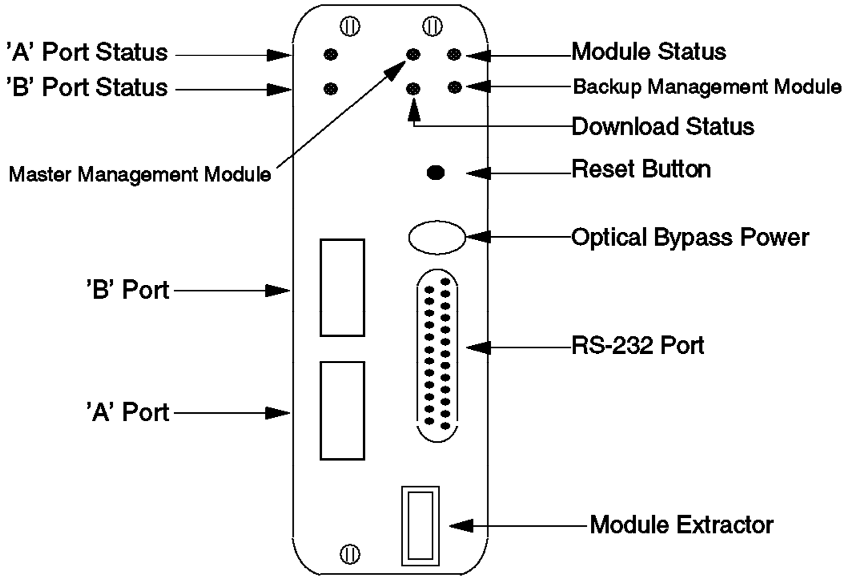


Figure 138. FDDI Management Module Front View

Table 51 describes the front panel LEDs on the FDDI management module.

Table 51. FMM LED Description

LED Name	Color	State	Description
A Port	Green	OFF	Port is disabled.
		ON	Port is enabled.
B Port	Green	OFF	Port is disabled.
		ON	Port is enabled.
Master Mgt Module	Green	OFF	FMM is a slave.
		ON	FMM is a master.
Status	Green	OFF	Powered down or not communicating with backplane or defective.
		ON	The power is on and the software is functioning properly.
Download	Yellow	OFF	The module is not downloading new software.
		ON	A download of new software is in progress.
Backup	Green	OFF	FMM is master.
		ON	FMM is slave.

11.2.3 Configuring the FMM

To configure the FDDI management module you should first configure your terminal to default FMM communication settings.

The default FMM settings are:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- Enable XOFF/XON

Once the terminal settings are done, you can use FMM to configure all the modules installed in the 8250. It is recommended that when using the FMM for the first time, you perform the following tasks:

- Establish passwords
- Set the internal clock
- Configure other FMM parameters
- Set FMM SNMP values
- Set FMM terminal for modem connection (optional)

Performing these tasks for FMM is very similar to that of EMM which is described in detail in 7.8.2, “ Configuring Ethernet Bridge Module” on page 171.

11.2.4 FDDI Topologies Using FMM

11.2.4.1 Tree Topology

In Figure 139 on page 271 we have set up a tree topology consisting of three 8250s using the A and B ports provided on the FDDI management modules. In this case, each 8250 can have up to a maximum of four FDDI fiber/STP modules.

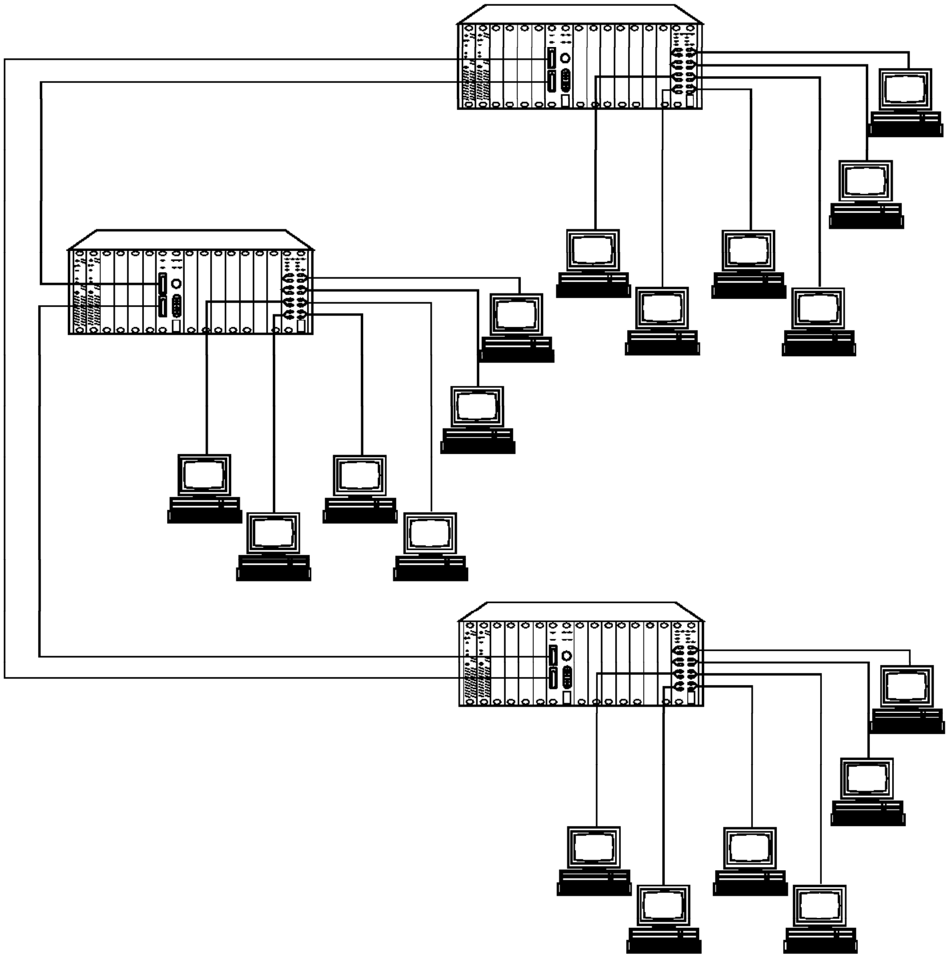


Figure 139. Tree Topology Using FDDI Management Module

11.2.4.2 Tree Topology

Figure 140 on page 272 shows an example where A and B ports on two FDDI management modules are used to build a dual-ring FDDI backbone.

In this example, the MAC stations on each FMM can be configured to run either on the primary or the backup ring. In addition, the FMM can be configured to connect either the primary or backup ring to the backplane, but not both. Therefore, the FDDI media modules on each 8250 may be connected to the main or the backup ring. Note that If you decide to connect the MAC on one FMM to the main ring and the other to the backup ring, each 8250 will form its own distinct ring and the stations on the two 8250s will be isolated from each other.

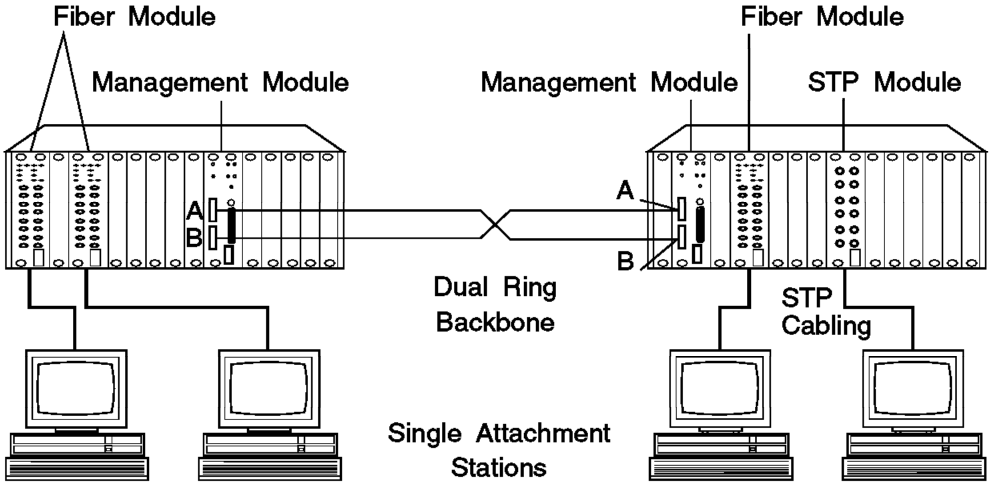


Figure 140. Dual Counter-Rotating Rings with FDDI Modules

For more examples of various possible and undesired configurations using the 8250 FDDI modules, refer to the documentation shipped with these modules.

Part 3. 8250 Management

Chapter 12. Hub Management - Before You Start

Before you begin to manage your network using AIX HMP/6000 there are a number of tasks that you need to address. These tasks are described in this chapter along with a description of the ITSC network environment used to test various scenarios in this and other chapters.

The following topics are addressed in this chapter:

- The ITSC Network
- Console Configuration
- SNMP Agent Configuration
- AIX NetView/6000 Configuration
- AIX HMP/6000 Configuration

You will need to have access to an asynchronous terminal console for these tasks.

12.1 The ITSC Network

As much of the material in the following chapters refers to and has been tested on the ITSC laboratory network; it will be useful for you to have a basic understanding of that environment.

The main components of the network include an 8250 Model 17, an 8250 Model 6 and an IBM RISC System/6000 network management station. In addition to this there were also numerous DOS and OS/2 PS/2 workstations, other RISC System/6000 hosts, and an 8209 token-ring to Ethernet bridge.

Although the network configuration changed many times throughout the project, essentially the IP network appeared as shown in Figure 141 on page 276.

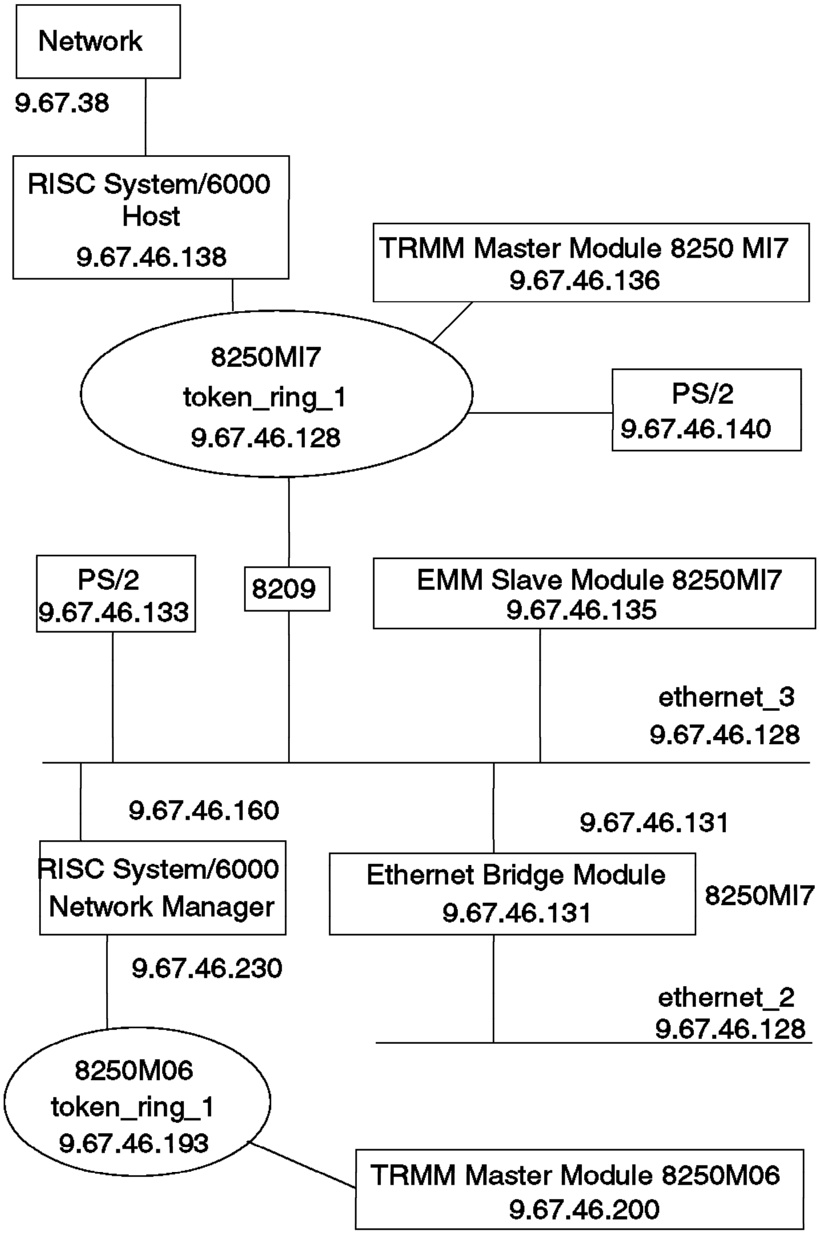
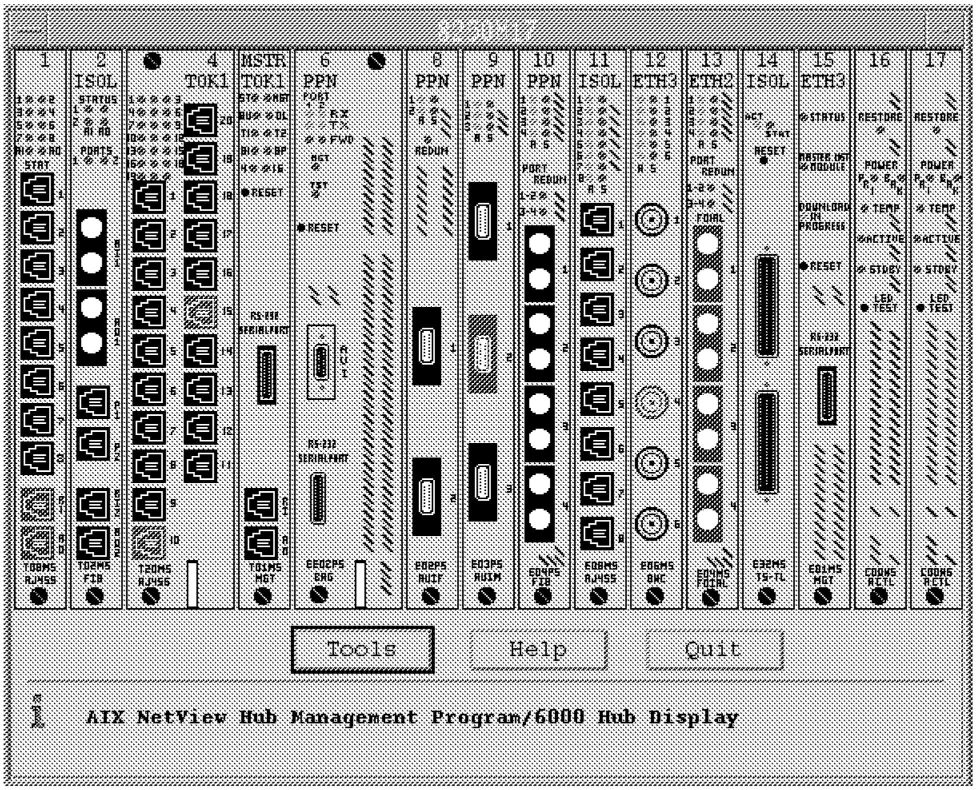


Figure 141. The ITSC Raleigh IP Network

Each of the 8250s were configured (primarily) as shown in the Hub Display Windows of AIX HMP/6000 as shown in Figure 142 on page 277 and Figure 143 on page 278.



AIX NetView Hub Management Program/6000 Hub Display

Figure 142. 8250M17. The 8250 Model 17 configuration.

The modules depicted in the 8250 Model 17 are shown in Table 52:

Table 52 (Page 1 of 2). The 8250 Model 17 Configuration

Slot	Module
1	Token-Ring Twisted Pair MAU
2	Token-Ring Fiber Repeater
3&4	Token-Ring Twisted Pair Media
5	Token-Ring Management
6&7	Ethernet Bridge
8	Ethernet Repeater
9	Ethernet Transceiver
10	Ethernet Four Port Fiber (Port Switchable)
11	Ethernet 10BASE-T (RJ-45)
12	Ethernet BNC
13	Ethernet Four Port Fiber (Non-Port Switchable)
14	Ethernet Terminal Server
15	Ethernet Management
16	Controller (Primary)

Table 52 (Page 2 of 2). The 8250 Model 17 Configuration	
Slot	**Module**
17	Controller (Backup)

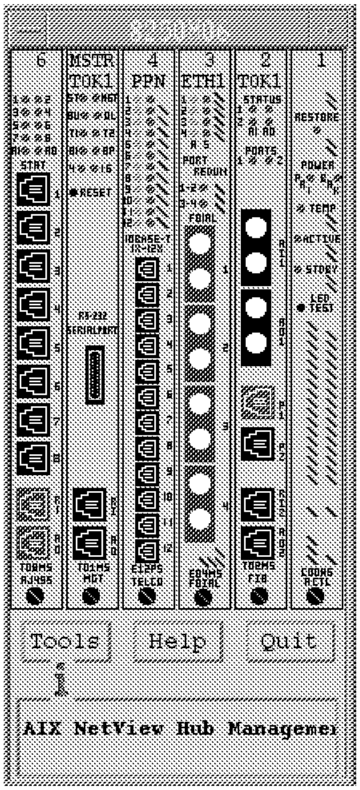


Figure 143. 8250M06. The 8250 Model 6 configuration.

The modules in the 8250 Model 006 were configured as shown in Table 53. Note that the modules in Figure 143 are displayed right to left.

Table 53. The 8250 Model 6 Configuration	
Slot	**Module**
1	Controller
2	Token-Ring Fiber Repeater
3	Ethernet FOIRL
4	Ethernet 12 Port 10BASE-T (Non-port switchable)
5	Token-Ring Management
6	Token-Ring Twisted Pair MAU

12.2 Console Configuration

The very first thing that you need to do, to enable management of your 8250 is to set up a terminal console. This is a requirement for both in-band and out-of-band management.

The reason a console is required for in-band management is two-fold:

- Before you can issue any in-band SNMP commands to your new 8250, you must first establish connectivity between the network management station (RISC System/6000) and the module agent (XMM). This requires you to set agent configuration parameters such as the IP address and subnet mask (see 12.3, "SNMP Agent Configuration" on page 281 for details).
- Even if SNMP is operating, not all MIB variables permit write access. For example, IP address can only be modified by out-of-band commands. Remember that out-of-band commands may be issued remotely provided the module you are managing supports Telnet (EMM and Ethernet Bridge module only support the proprietary remote_login, which allows remote login from another module which supports remote_login).

The token-ring management module, the Ethernet management module, FDDI management module, token-ring bridge module, Ethernet bridge module and the terminal server module have the capacity to support a direct RS-232 attached ASCII terminal console. Note that in the case of terminal server, there is no RS-232 port on the module and the ASCII terminal is normally connected via a Harmonica to the Telco connector on the module.

This section will cover initial terminal attachment and the factory default settings, how to change the factory default settings using out-of-band commands and how to change the port parameters using in-band management via AIX HMP/6000.

12.2.1 Initial Console Attachment

When you initially attach your console terminal to your IBM 8250 Multiprotocol Intelligent Hub, you must ensure that your terminal′s communications parameters are equivalent to the factory default settings for the module you are connecting to. If you are unsure of the current settings of your terminal, consult the documentation supplied with the terminal for information on how to view and modify its configuration.

The token-ring management module RS-232 port communications parameters are factory set to the values shown in Table 54.

Table 54. The Token Ring Management Module RS-232 Port Factory Set Defaults

Port Parameter	Factory Set Value
baud rate	9600
data bits	8
parity	none
stop bits	1

The Ethernet management module and Ethernet bridge module both have RS-232 port factory default settings as shown in Table 55 on page 280.

Table 55. The Ethernet Management and Bridge Module RS-232 Port Defaults

Port Parameter	Factory Set Value
baud rate	9600
data bits	8
parity	none
stop bits	2

If you are managing an environment with a mix of token-ring management modules and Ethernet management modules we suggest that you alter the *stop bit* parameter so they are consistent between the token-ring management module and the Ethernet modules. This will prevent you from having to change your terminal setup every time you wish to switch between the modules. Of course this is only the case where you have only one console terminal.

12.2.2 Terminal Configuration Using Out-of-Band Management Commands

Once you have established connectivity with your console you can change the configuration parameters of the RS-232 port if you desire.

To do this, from the console itself, use the `set terminal` command for each parameter you wish to alter. Refer to the documentation supplied with your module for more information on this command.

Note that the effect of issuing the *set terminal* command is immediate. That is, the set up of your terminal will no longer be equivalent to the RS-232 port configuration and you may lose your connection. This will happen if you reset either the *baud rate*, the number of *data bits* or the *parity* parameter for the terminal port.

To re-establish the connection simply modify your terminal setup to be consistent with the changes you made and hit the *enter* key on your keyboard. This will reconnect the session without you having to re-login.

Make sure you save your changes when you are finished. To do this simply issue the command:

```
save terminal
```

12.2.3 Terminal Configuration Using In-Band Management via AIX HMP/6000

Although you will not be able to use *in-band* management until IP connectivity has been established, (see later in this chapter), we have included in-band terminal configuration here because it is relevant to configuration of the console.

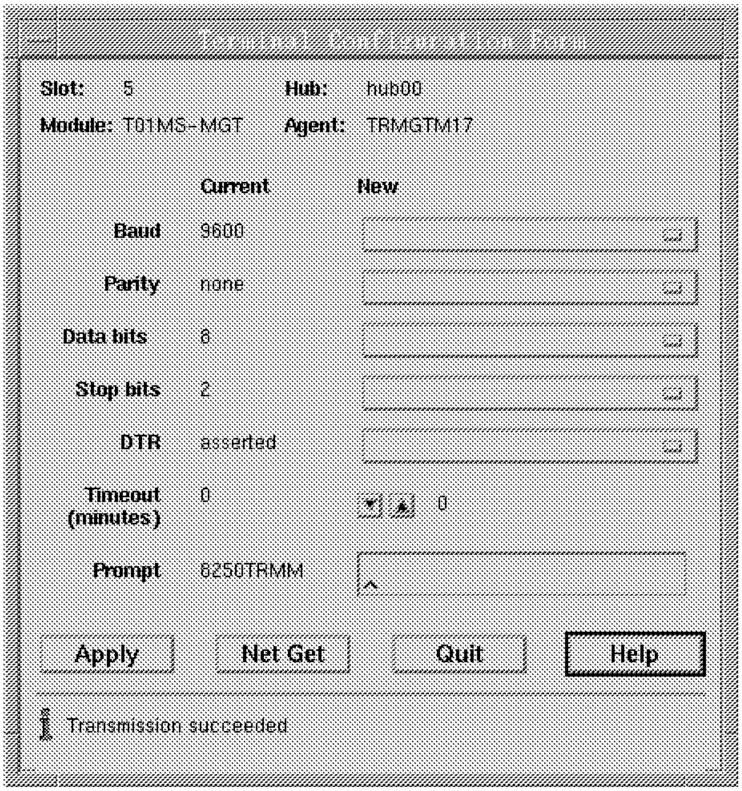
Note

Currently the Ethernet bridge module does not support in-band configuration of its RS-232 port.

The process for configuring the RS-232 port parameters for the token-ring management module and the Ethernet management module is identical.

12.2.3.1 An Example of In-Band Terminal Configuration

From the AIX HMP/6000 Hub Display window, see Figure 142 on page 277, clicking on the RS-232 port on either the token-ring management module or Ethernet management module will invoke the **Terminal Configuration Form** similar to that shown in Figure 144.



Terminal Configuration Form

Slot: 5 Hub: hub00

Module: T01MS-MGT Agent: TRMGTM17

	Current	New
Baud	9600	
Parity	none	
Data bits	8	
Stop bits	2	
DTR	asserted	
Timeout (minutes)	0	0
Prompt	8250TRMM	

Transmission succeeded

Figure 144. The Terminal Configuration Form

It is more convenient to change the console configuration using the in-band management form because you can change multiple port parameters with a single application of the form as opposed to issuing multiple out-of-band port commands and reconfiguring the terminal after each one.

12.3 SNMP Agent Configuration

For each token-ring management module, Ethernet management module, Ethernet terminal server module and Ethernet bridge module that you wish to manage via AIX HMP/6000, you must configure the following information:

- IP address
- Subnet mask
- Community access

Additionally, depending on your network design, you may also need to configure the default gateway parameter.

The following instructions are relevant to the token-ring management module, Ethernet management module and the Ethernet bridge module. Configuration of the Ethernet terminal server module is significantly different from these modules. Please refer to Chapter 8, “Ethernet Terminal Server Module” on page 189 or the *Ethernet Terminal Server Reference Manual* for configuration information on this module.

12.3.1 IP Address Configuration

To configure the IP address on an SNMP agent module you will need to execute the **set device ip_address** command. This command must be entered from a terminal attached to the module itself or from a remote login session, provided you are logged on as the administrator. Obviously for initial setup you will need to execute this from a direct-attached console. You cannot execute a set device command from a management module to another agent, even if you are the master.

As an example, to configure the IP address for the Ethernet management module in the 8250 Model 17 on our network, we entered the following:

```
set device ip_address 9.67.46.135
```

When we tested this command using a Telnet session to a token-ring management module, the session was preserved.

12.3.2 Subnet Mask Configuration

Similarly, to configure the subnet mask, you will need to execute the set device subnet_mask command.

Again using the Ethernet management module in our example network we entered:

```
set device subnet_mask FF.FF.FF.C0
```

The subnet mask must be entered in hexadecimal format.

12.3.3 Community Access Configuration

A **community name** must be configured for each SNMP agent module that you want to manage using AIX HMP/6000. This parameter is used to control access to the SNMP agent by the network management workstation(s).

To configure the community name *ITSC* for the Ethernet module in slot 15, allowing both read and write access to a network manager (9.67.46.160) on the network, enter the following command at the terminal console:

```
set community ITSC 9.67.46.160 all
```

You have the capability to control the access permissions that are granted to the specified IP address. The following list specifies the access options:

- *trap* access means that the specified IP address will receive only traps (alerts) from the specified agent.
- read_trap access means that the specified IP address can display information about the agent and it will receive traps.
- read_only access means that the specified IP address can only display information about the agent.

- read_write access means that the specified IP address can display and modify information about the agent.
- all access means that the specified IP address has both read_write and trap access. This is the access we granted in the example shown above.

Community name access must be configured for both the SNMP agent and the SNMP network management station. 12.4, “AIX NetView/6000 Configuration” details the process required to configure the community name on the AIX NetView/6000 network manager.

12.3.4 Gateway Configuration

If you wish to manage modules on different IP networks you will need to set the default_gateway parameter for your management module(s).

A separate gateway may be configured for each of the networks that your management module can connect to. For the Ethernet management module, a gateway can be configured for ETHERNET1, 2 and 3 or you can simply configure just one gateway and assign it to all three Ethernet networks.

For the token-ring management module, a separate gateway can be configured for each of the 7 possible token rings or equally one gateway may be assigned to all. Additionally, the token-ring management module supports a gateway in isolated mode as it may communicate to another IP network via its RI/RO ports.

To set the default gateway you must enter the following out-of-band command at the console:

```
set device default_gateway 9.67.46.160
```

12.4 AIX NetView/6000 Configuration

After AIX NetView/6000 and AIX HMP/6000 have been installed, the following tasks need to be executed:

1. Load the ibm-8250.mib file.
2. Edit the oid_to_type file.
3. Edit the /etc/community file.

12.4.1.1 Load the ibm-8250.mib File

1. From the **Configure** menu on the AIX NetView/6000 console, select the **Load/Unload MIBs** option.
2. If applicable, be sure to unload any Chipcom MIB before proceeding.
3. Select the */usr/etc/nm/mibs/examples* directory from the input list and load the *ibm-8250.mib* file.

12.4.1.2 Edit the oid_to_type File

Add the following entries to the oid_to_type file:

```
1.3.6.1.4.1.49.2.3.5: 0x02000002 # IBM 8250 (EMM)

1.3.6.1.4.1.49.2.3.7: 0x02000002 # IBM 8250 (TRMM)

1.3.6.1.4.1.49.2.3.2: 0x02000004 # IBM 8250 (EBM)

1.3.6.1.4.1.85:       0x04000002 # IBM 8250 (ETS)
```

12.4.1.3 Edit the /etc/community File

For each unique agent community name, a corresponding entry needs to be declared in the network manager if that agent is to be managed. This is done in the AIX NetView/6000 file, /etc/community.

The community file contains a list of paired entries in the following format:

```
agent community
```

Any SNMP request for an *agent* listed in this file will be sent with the corresponding *community* entry. On receipt of the request, the agent will process the request according to the permissions it has configured for that community name. If an invalid community name is sent, the agent will generate an authentication failure trap.

There is a special entry, called the *default*, which may be used for any agent which does not have a specific entry in the file. For example, as all the agents in our network used the community name ITSC, our /etc/community file contained only one entry as follows:

```
default ITSC
```

This means that all SNMP requests in our network were sent with a community name of ITSC.

If there is no default entry in the file and an application cannot find a match for a specific agent then the SNMP request will be sent with a community name of *public* The community name *public* should not be used for specific agents for this reason.

12.5 AIX HMP/6000 Configuration

The hmp.cfg file only contains information about hubs, agent modules and ports.

General Rules

- Each line may contain up to 256 characters.
- An *identifier* can be up to 20 characters and must not contain blanks.
- Keywords must be in lowercase.
- Hub names can be up to 12 characters in length.
- Identifiers must be separated by a blank.
- Comments begin with an exclamation mark (!) and can start anywhere on any line.
- Any line may be left blank.
- Lines that are not blank or are not comments must begin with a keyword and must include all parameters related to that keyword.

Hubs

- At least one hub must be declared in the file.
- Each hub declaration must begin with the keyword **hub**, followed by a space and the name of the hub.

- The names of hubs can be chosen arbitrarily but they must not contain blanks.
- All hubs to be managed must be declared.
- The default hub type is *8250-017*. If you are managing a different model, such as a Model 6 hub, the *name* should be followed by a space and a type identifier in the *type* field.

Modules

- Each module declaration must begin with the keyword **module**, followed by the host name of the agent, a space and the module type identifier.
- The names of modules should be the agent names you have defined for AIX NetView/6000 in the */etc/hosts* file.
- The current identifiers are:
  - Token-ring management module - T01MS-MGT
  - Ethernet management module - E01MS-MGT
  - Ethernet bridge module - EE02PS-BRG
  - Ethernet terminal server module - E32MS-TS-T or E32MS-TS-TL
- All management modules must be declared.
- Each hub must have at least one management module.
- Any agent module may be specified.
- Up to 6 management modules may be specified for each hub and/or as many bridges or terminal servers as you wish.

Ports

- Port declarations are optional. They provide additional information that the system manager can display using the *Information* forms.

  Each port declaration must begin with the keyword **port**, a space, the slot number, a period (.), the port number, a space and an optional description.
- The description is free format text.

12.5.1 A Sample Configuration File

The following sample is the hmp.cfg file that we used. We did not have any port declarations.

```
! Wed Mar 3 09:38:41 EST 1993

hub 8250M17 8250-017

module TRMGTM17 T01MS-MGT    ! master Slot=5 MAC=08-00-8F-F0-E0-C3
module EMGTM17 E01MS-MGT     ! non-master Slot=15 MAC=08-00-8F-10-33-63
module EBRIDGE EE02PS-BRG    ! non-master Slot=6 MAC=08-00-8F-10-30-10

hub 8250M06 8250-006

module TRMGTM06 T01MS-MGT    ! master Slot=5 MAC=08-00-8F-F0-10-54

! End of configuration file.
```

Chapter 13. AIX NetView Hub Management Program/6000

This chapter describes the AIX NetView Hub Management Program/6000 or AIX HMP/6000 for short. The sections covered in this chapter are:

- A Product Description
- The Components of AIX HMP/6000
- The AIX HMP/6000 Database and Browser Utility
- AIX HMP/6000 Internals
- Using AIX HMP/6000
- Installation Experiences

13.1 Product Description

The IBM 8250 Multiprotocol Intelligent Hub can be managed by any of the following methods, (or a combination of them):

1. Via an asynchronously attached ASCII terminal. This is referred to as **out-of-band** management.
2. Using an SNMP manager which communicates with the 8250 management modules, over a TCP/IP network. This is referred to as **in-band** management.
3. Using a remote terminal to login to the management module (except EMM), using Telnet, to manage the 8250 remotely.

AIX HMP/6000 is an SNMP-based application that implements *in-band* management of the IBM 8250 Multiprotocol Intelligent Hub. It is an end user application which also uses the functions of AIX NetView/6000 via application programming interfaces (APIs). At the time of writing, AIX HMP/6000 Version 1.0 is only supported under AIX NetView/6000 Version 1.0.

AIX HMP/6000 uses a number of AIX NetView/6000 features. It uses the autodiscovery feature of AIX NetView/6000 to *learn* about the 8250 agents reachable. It uses the AIX NetView/6000 trap monitoring process to collect unsolicited information from the 8250 agents. AIX HMP/6000 also relies on information stored in the AIX NetView/6000 topology database to keep much of its own configuration information current.

AIX HMP/6000 provides a graphical user interface for monitoring and managing the modules installed in the IBM 8250 Multiprotocol Intelligent Hub. Like AIX NetView/6000, AIX HMP/6000 uses color-coded status indicators to greatly simplify network monitoring by the operator.

The AIX HMP/6000 graphical user interface (GUI) supports interfaces at both the *hub* and *module* levels. These windows support a series of mouse-driven menus which can be used to invoke a series of *forms* which facilitate operations on hubs, modules and ports. Statistical monitoring operations are also supported.

AIX HMP/6000 also includes a menu-driven utility which allows you to centralize and cross reference specific information about your network. This is known as the *Browser* utility. The Browser automatically stores information that is gathered during autodiscovery. Additionally the network administrator can add other relevant user and site specific information.

13.2 The Components of AIX HMP/6000

This section lists the primary files, daemons and executables (shell scripts and compiled programs) of AIX HMP/6000 and provides a brief explanation of each.

13.2.1 AIX HMP/6000 Product Files

/usr/etc/hmp/app-defaults/Hmp

A flat file containing the X resources for AIX HMP/6000

/usr/etc/hmp/helps/Hmp

A directory containing the AIX HMP/6000 help files

/usr/etc/hmp/strings/Hmp

A directory containing the AIX HMP/6000 message files

/usr/etc/hmp/uid/Hmp

A directory containing the AIX HMP/6000 GUI definitions

13.2.2 AIX HMP/6000 Daemons

hmpf1d

An RPC server daemon which provides access to the AIX HMP/6000 database.

hmpsnmpd

Receives trap and event information via an API from AIX NetView/6000.

Forwards SNMP requests directly to 8250 agents.

hmpmond

The hmpmond daemon monitors traps via the hmpsnmpd daemon and updates the database accordingly if so dictated by the trap information it receives. It also periodically polls the 8250 agents to remain current with their configuration details. SNMP requests generated from hmpmond are also transmitted via hmpsnmpd.

If hmpmond receives a trap indicating that a new agent has come online or an existing agent has failed, then it will adjust its polling to reflect this.

xhmp

The AIX HMP/6000 end user GUI interface daemon. A client of the hmpf1d daemon.

adtmd

Responsible for monitoring event and trap information from AIX NetView/6000 related to major configuration changes in the hub.

13.2.3 AIX HMP/6000 Other Executables

adcfg

A shell script which generates the AIX HMP/6000 configuration file, */usr/etc/hmp/data/hmp.cfg*.

hmp6000

A shell script which is used to start AIX HMP/6000. When there is difficulty in starting one or more AIX HMP/6000 daemons, this file can be edited to remove the /dev/null redirected printout to discover the reason for failure.

hmpmf1upd

This shell script updates the AIX HMP/6000 database with *machine* information which it obtains by parsing the AIX NetView/6000 topology database.

The AIX *cron* daemon invokes hmpmf1upd every 15 minutes.

hmpuf1upd

This shell script updates the AIX HMP/6000 database with *user* information.

User information is added explicitly via the AIX SMIT tool. When the corresponding SMIT command is run, hmpuf1upd is invoked.

hmpf1cl

An executable command line interface for the *hmp6000_smit* command and the hmpmf1upd and hmpuf1upd daemons.

The hmpf1cl executable is a client of the hmpf1d server daemon.

browser

The browser program is also a client of the hmpf1d daemon and is responsible for displaying the AIX HMP/6000 browser user interface window.

ibm6611_fe

An hmpf1d client responsible for displaying the AIX HMP/6000 6611 user interface window.

hmp6000_smit

Invoked when HMP/6000 is specified from SMIT.

13.3 The AIX HMP/6000 Database

This section describes the AIX HMP/6000 database and **Browser** utility.

13.3.1 The Database

The AIX HMP/6000 database allows you to group related network information for easy reference. This may be useful in a scenario where you are managing environments comprised of autonomous or semi-autonomous components such as user work groups or network segments, for example.

There are three group structures supported within the database. These are termed operational **modes**. Each mode cross references information with the others. The three modes are:

- Machines
- Hubs

- Users

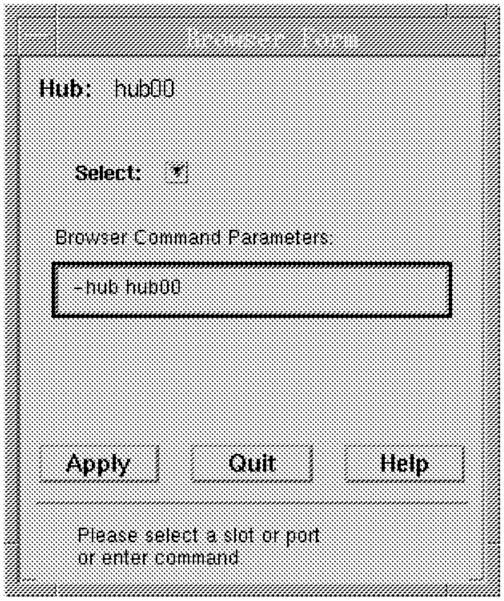
Machine and **Hub** information is automatically added to the database using information supplied via the AIX NetView/6000 autodiscovery feature. This information is updated by the AIX NetView/6000 topology database and the AIX HMP/6000 hmpmond daemon.

User information must be updated manually via the AIX SMIT utility.

13.3.2 The Browser Utility

The **Browser** utility is the AIX HMP/6000 user interface to the database. It provides tools for both general enquiry access and maintenance of the database.

The *Browser* form shown in Figure 145 can be invoked from the *Tools* menu on the AIX HMP/6000 Hub Display window.



Hub: hub00

Browser Command Parameters:

-hub hub00

Please select a slot or port
or enter command

Figure 145. The Browser Form

The Browser form supports the following commands which allow the database to be opened at a specific location:

```
-user {username|usergroup}
-machine {machinename|machinegroup}
-hub {hubname {-slot slotnumber {-port portnumber}}|hubgroup}
```

In the above notation, brackets {} denote options and the vertical bar denotes *or*. The *username, usergroup, machinename etc.* are user-defined parameter information.

Once the desired command has been entered in the Browser form, it can be executed by clicking on the **Apply** button. This will invoke the *Browser Selection* screen which will look similar to the one shown in Figure 146 on page 291.

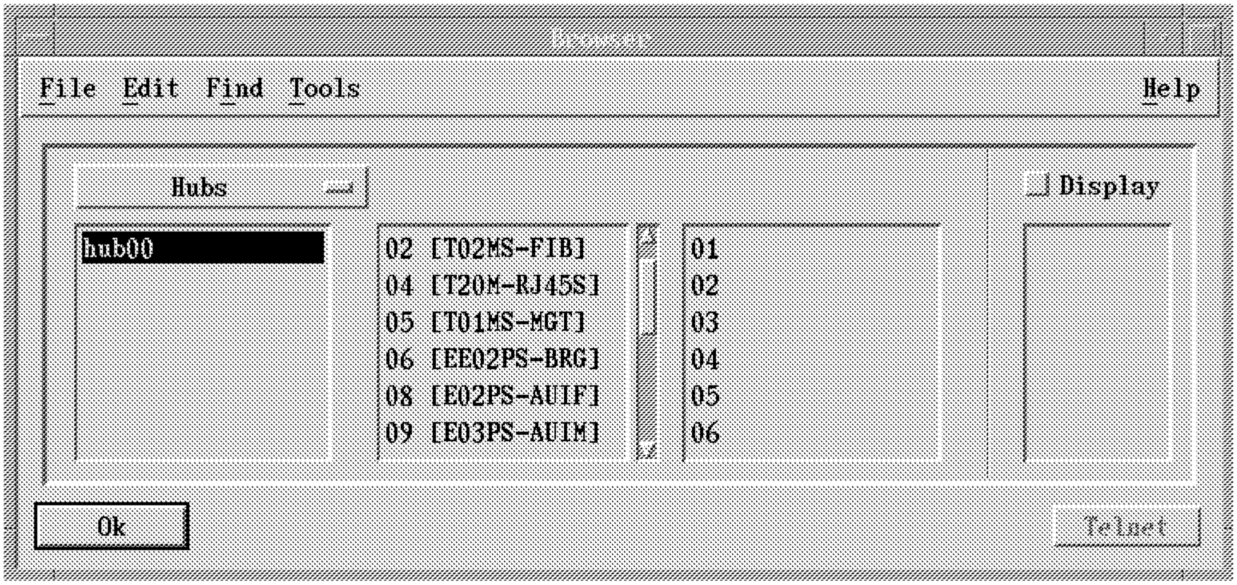


Figure 146. The Browser Selection Screen

This display shows the hub information for *hub00*. This is one of the default groupings that are set automatically by the database. You can define your own groups which may refer to any list of specific users, machines, hubs, modules or ports. Groups may also refer to other groups.

There is also a special group which is common to all Browser selection screens called the **defaults** group. This group is created automatically to store information which is obtained via autodiscovery. The information in the defaults group can be transferred to another group if desired. The procedure for doing this is outlined in the AIX HMP/6000 documentation.

As explained previously, information is stored in the database according to a *mode*. The mode button in the Browser Selection screen allows you to select the mode of operation that you want to work with.

13.3.2.1 The Browser Utility Menus

There are a series of *pull-down* menus available for managing the database. These are explained in this section.

The File Menu

This menu is used to exit the Browser utility. Exiting via this menu automatically saves all changes.

The Edit Menu

This menu provides access to a number of forms which enable read and write access to the database. The options available under this menu are as follows:

View

This option allows read-only access to the Entry Form for a highlighted item or group.

Modify

Use the modify option to invoke a form for a highlighted item or group to which you wish to make changes.

Create Item

Use this option to add a new item to an existing group.

Create Group

This option can be used to add a new group to an existing group.

Delete

The delete option removes an item or a group from the database.

The AIX HMP/6000 documentation provides more information on the forms invoked from this menu.

The Find Menu

The Find menu enables you to locate components of the database. The item or group that you specify must be linked to the same menu *mode* as that which you have open at the time you invoke the *find* request.

The following are valid search arguments for the find tool:

- Item or group name
- IP address
- MAC address
- The *top* level of an ancestry

13.4 AIX HMP/6000 Internals

This section explains the internal workings of AIX HMP/6000 and its primary interfaces with AIX NetView/6000 and the IBM 8250 Multiprotocol Intelligent Hub. A diagram showing the various components of AIX NetView/6000 and AIX HMP/6000 and their relationship can be seen in Figure 147 on page 293.

13.4.1 The hmp.cfg Configuration File

The hmp.cfg file contains the configuration information used by the AIX HMP/6000 application. Only the information declared in this file can be displayed or accessed via AIX HMP/6000. The core AIX HMP/6000 daemon, *xhmp*, uses the hmp.cfg file to validate the Console icons, which it can present to the user, and to build the subsequent Hub Display windows.

Mostly, this file is generated automatically using the information gathered by the AIX HMP/6000 autodiscovery process. This data is collected by AIX NetView/6000 and stored in the AIX NetView/6000 topology database. The AIX HMP/6000 shell script **adcfg**, retrieves relevant 8250 hub configuration information from this database and uses it to create, or re-create, the hmp.cfg file.

The adcfg shell script can be explicitly invoked by the root user, if required, by selecting the *Discovery/Load* option under the *File* menu of the AIX HMP/6000 console. This may be required when there is a major configuration change in the hub.

The hmp.cfg file can also be manually edited from the AIX SMIT utility. This option simply invokes a *vi* edit session on hmp.cfg.

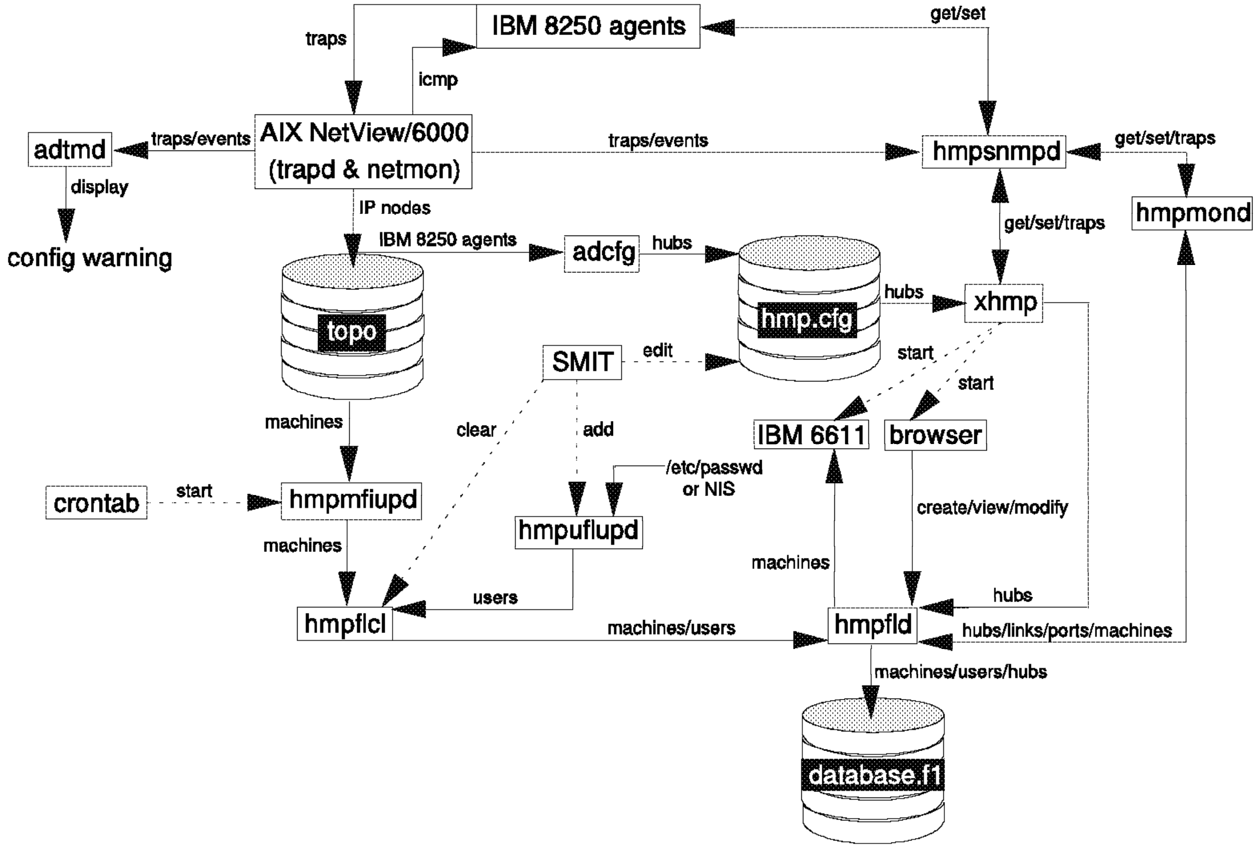


Figure 147. AIX HMP/6000. The logical interfaces of AIX HMP/6000, AIX NetView/6000 and the IBM 8250 Multiprotocol Intelligent Hub.

13.4.2 Traps and Events

The monitoring and reporting of traps received from the 8250 SNMP agents is facilitated by AIX NetView/6000. The AIX HMP/6000 daemon process **hmpsnmpd**, interacts with the AIX NetView/6000 **trapd** daemon via an application programming interface (API) to transfer 8250 trap information to the AIX HMP/6000 application.

Note that the *hmpsnmpd* daemon is not an SNMP agent process as is its AIX NetView/6000 namesake, *snmpd*.

Remember that AIX HMP/6000 is *not* an SNMP manager in its own right. AIX HMP/6000 is a specific management application that uses the services of a generic network manager, AIX NetView/6000. It does not make sense to duplicate the community name and trap configuration information that is already encompassed in AIX NetView/6000.

Once traps are received, hmpsnmpd is responsible for forwarding this information to two other AIX HMP/6000 daemons. These are the **hmpmond** and **xhmp** daemons.

The *hmpmond* daemon regularly polls the 8250 agents to monitor the status and configuration of all the hub modules, including the non-agent modules. It has a default polling period of 30 minutes. All SNMP interactions between hmpmond and the 8250 hub are implemented via hmpsnmpd.

When hmpmond detects any changes it updates the AIX HMP/6000 database via the hmpf1d daemon.

When the hmpmond daemon detects any of the following traps it will re-adjust its polling appropriately to either include the newly detected device or to prevent unnecessary polling:

- ColdStart
- WarmStart
- SlotUp
- SlotDown

The *xhmp* daemon presents the trap information to the end user. An example may be an error message displayed in the *information* section of an AIX HMP/6000 window.

When the trap results from a major change to the configuration of the hub, another daemon called **adtmd** comes into consideration.

The addition or removal of a module to/from a hub, often requires that the configuration file, hmp.cfg, be regenerated. The AIX HMP/6000 daemon *adtmd* is responsible for warning the end user of this. When such an event occurs a new window is opened containing a warning to this effect.

The *adtmd* daemon can be notified of these events by one of the following two sources:

- Via a trap sent to the AIX NetView/6000 trapd daemon from the 8250 management module or
- The AIX NetView/6000 daemon netmon, when a management module is not present in the hub

The configuration file can then be explicitly regenerated by selecting the *Discovery/Load* option under the *File* menu of the AIX HMP/6000 Console window.

13.4.3 SNMP Requests

All AIX HMP/6000 SNMP requests are passed to the **hmpsnmpd** daemon which is, in turn, responsible for forwarding them directly to the 8250 agent.

SNMP requests are generated regularly by the AIX HMP/6000 monitoring daemon, **hmpmond**, or they may be generated from xhmp randomly as a direct result of a user action.

Of course, standard SNMP requests can be issued from the AIX NetView/6000 Browser tool or even the AIX command line; however, those requests issued from AIX HMP/6000 are not passed via AIX NetView/6000. This is because AIX NetView/6000 is a generic network manager and does not, by design, provide specific SNMP management functions. That is the role of applications such as AIX HMP/6000.

In addition to supporting standard SNMP commands, AIX HMP/6000 also provides user interface enhancements such as specialized *forms* which consolidate information relevant to the agent being queried and graphical representations of statistical data.

13.4.4 The AIX HMP/6000 Database - Behind the Scenes

The AIX HMP/6000 database maintains its information from many different sources. We have already discussed how the Browser utility can be used to create relationships between information in the database and to maintain this data. This section will look at a number of other AIX HMP/6000 daemon processes that also maintain the information in the database.

AIX HMP/6000 uses the AIX NetView/6000 topology database, */usr/etc/nm/databases/topo_db*, to find information about *machines* in the network. The shell script **hmpmf1upd** is invoked via a cron entry every 15 minutes to read the AIX NetView/6000 topology database and extract the machine information relevant to AIX HMP/6000.

This *machine* information is then forwarded to the AIX HMP/6000 database process, **hmpf1cl**. The *hmpf1cl* process is a client process of the **hmpf1d** daemon which directly accesses the AIX HMP/6000 database.

The *hmpf1cl* client also accepts *user* information from the **hmpuf1upd** daemon which it (hmpf1cl) then passes to the *hmpf1d* database server daemon.

User information may be passed to the *hmpuf1upd* daemon via explicit commands that are executable from the AIX HMP/6000 SMIT menus.

Both the SMIT and Browser utilities can be used to clear information from the database.

13.5 Using AIX HMP/6000

There are two main starting points for all AIX HMP/6000 operations. These are the **Console** window and the **Hub Display** window.

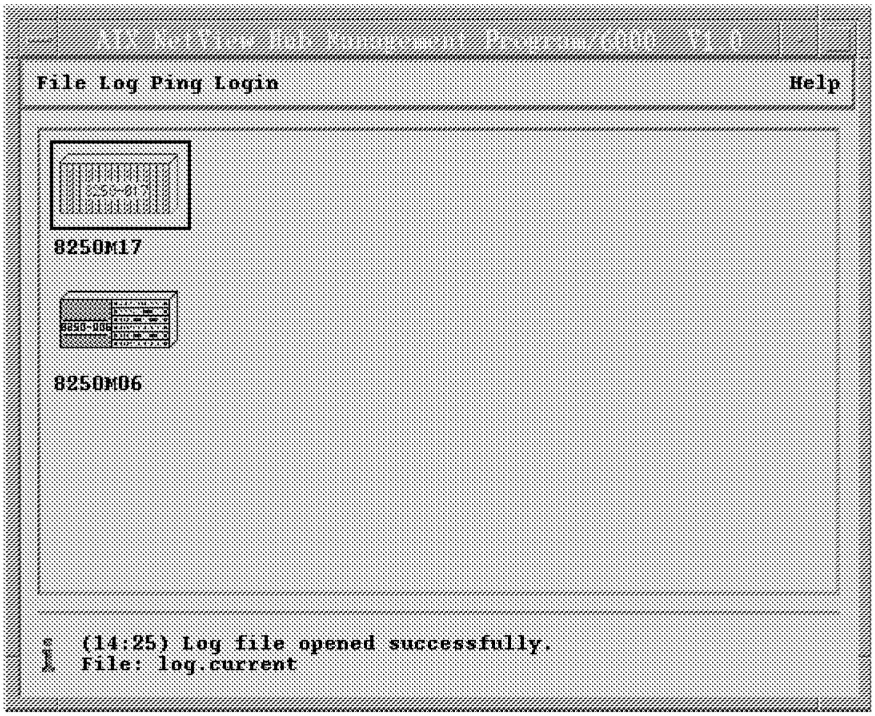
The Console window is for the selection of individual hubs to manage and general management tools.

The Hub Display window is used for management operations on individual modules and networks.

For all operations, the mouse is the primary input tool and almost always, the left mouse button only.

13.5.1 The AIX HMP/6000 Console

The Console window provides overall management facilities for AIX HMP/6000.



```
(14:25) Log file opened successfully.
File: log.current
```

Figure 148. The AIX HMP/6000 Console Window

As can be seen in Figure 148 the Console window includes three main sections:

- Menu bar
- Work area
- Information area

The central **work area** depicts all hubs detected by the AIX HMP/6000 discovery process and those represented in the configuration file. There are different icons for the Model 6 and Model 17 8250 hubs.

The color of each icon indicates the status of AIX HMP/6000′s connectivity to that hub. All hubs are initially depicted blue. Green hubs are currently manageable by AIX HMP/6000. A hub is displayed red if AIX HMP/6000 polls it but fails to establish a connection or the program loses communication with the hub.

The **menu bar** supports the following operations:

The File Menu

The following operations are available under the *File* menu:

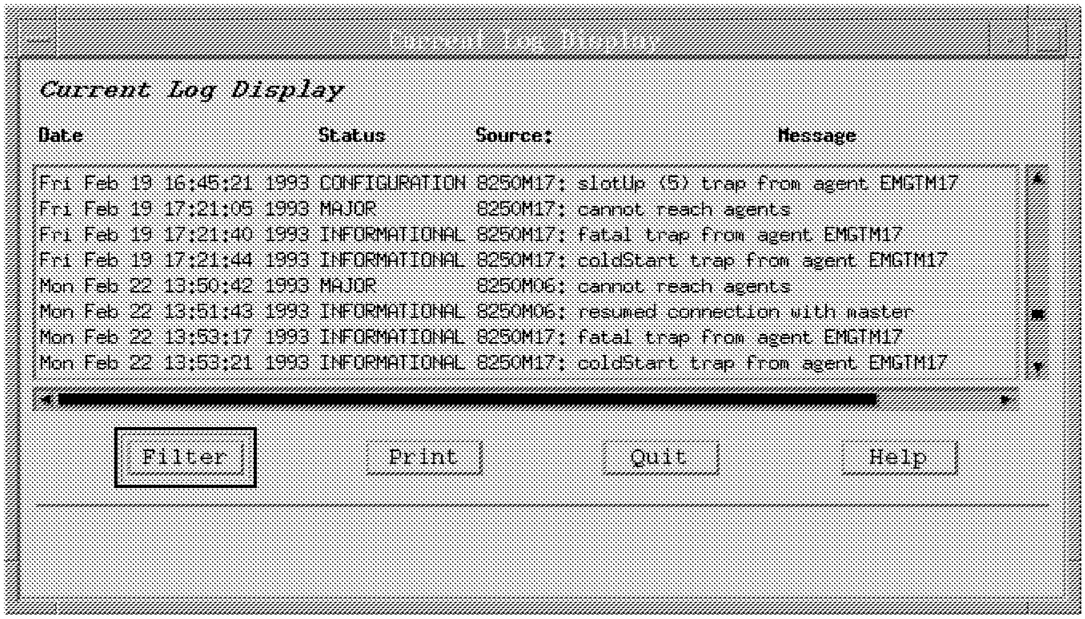
- **Load** - use to reload the configuration file whenever it has been explicitly edited. The work area will be recreated as a result.
- **Discovery/Load** - use to regenerate the configuration file; AIX HMP/6000 usually prompts you when this is necessary. The present configuration file is erased and the Netview/6000 topology database is searched anew for 8250 hubs.
- **Quit** - use to exit AIX HMP/6000.

The Log Menu

AIX HMP/6000 records warning and informational messages in its *log.current* file in the current working directory by default.

The *Log* menu allows you to:

- **Display** a continuously updated log.
- **Browse** previously saved log files.
- **Save** the current log file and clear the log.



```
Date                       Status         Source:                    Message
Fri Feb 19 16:45:21 1993 CONFIGURATION 8250M17: slotUp (5) trap from agent EMGTM17
Fri Feb 19 17:21:05 1993 MAJOR         8250M17: cannot reach agents
Fri Feb 19 17:21:40 1993 INFORMATIONAL 8250M17: fatal trap from agent EMGTM17
Fri Feb 19 17:21:44 1993 INFORMATIONAL 8250M17: coldStart trap from agent EMGTM17
Mon Feb 22 13:50:42 1993 MAJOR         8250M06: cannot reach agents
Mon Feb 22 13:51:43 1993 INFORMATIONAL 8250M06: resumed connection with master
Mon Feb 22 13:53:17 1993 INFORMATIONAL 8250M17: fatal trap from agent EMGTM17
Mon Feb 22 13:53:21 1993 INFORMATIONAL 8250M17: coldStart trap from agent EMGTM17
```

Figure 149. The AIX HMP/6000 Log Display Window

As can be seen from Figure 149, the log displays the date, status priority, the source and the contents of each message. The following message categories are available:

- Informational

  These messages usually indicate normal or expected events and do not require any intervention by the operator.

- Minor

  Minor messages usually indicate temporary communications problems. If they persist, operator intervention is required.

- Major

  Major messages are generated if AIX HMP/6000 fails to successfully open a hub. The hub cannot be managed until the problem is rectified.

- Configuration

  These messages indicate a change in the configuration of the hub.

- Security

Security messages indicate that another manager has been, or is attempting to manage, the hub at the same time.

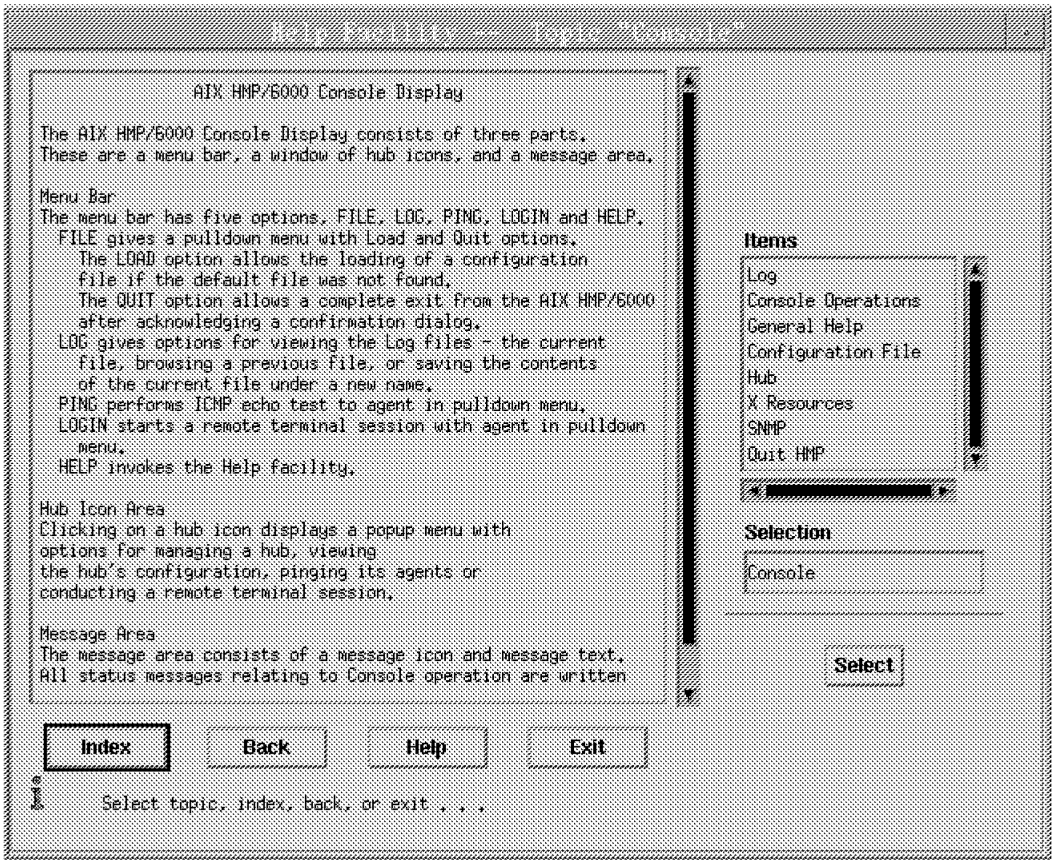
A complete list of messages can be found in the AIX HMP/6000 manual.

The **Log filter** is a facility which can be used to selectively choose those messages which are to be included in the log.

The **Ping** and **Login** menus are self-explanatory.

The Help Menu

The Help facility of AIX HMP/6000 is a context sensitive tool. That is, when selected, help displays a window of information about the form from which it was invoked. Figure 150 shows the help facility invoked from the Console window.



```
                 AIX HMP/6000 Console Display

The AIX HMP/6000 Console Display consists of three parts.
These are a menu bar, a window of hub icons, and a message area.

Menu Bar
The menu bar has five options, FILE, LOG, PING, LOGIN and HELP.
  FILE gives a pulldown menu with Load and Quit options.
    The LOAD option allows the loading of a configuration
    file if the default file was not found.
    The QUIT option allows a complete exit from the AIX HMP/6000
    after acknowledging a confirmation dialog.
  LOG gives options for viewing the Log files - the current
    file, browsing a previous file, or saving the contents
    of the current file under a new name.
  PING performs ICMP echo test to agent in pulldown menu.
  LOGIN starts a remote terminal session with agent in pulldown
    menu.
  HELP invokes the Help facility.

Hub Icon Area
Clicking on a hub icon displays a popup menu with
options for managing a hub, viewing
the hub's configuration, pinging its agents or
conducting a remote terminal session.

Message Area
The message area consists of a message icon and message text.
All status messages relating to Console operation are written
```

```
      Select topic, index, back, or exit . . .
```

Figure 150. The AIX HMP/6000 Help Display Window

AIX HMP/6000 reserves the bottom of each window or form as an **Information Area**. This area is used for displaying AIX HMP/6000 messages which usually indicate temporary conditions in the hub, normal or expected changes of state, or the correction of a problem. Usually, these messages are purely informational and do not require intervention by the operator. A descriptive list of AIX HMP/6000 messages can be found in the AIX HMP/6000 manual.

There are three symbols associated with AIX HMP/6000 messages:

1. The **i** symbol indicates a normal operational message.
2. The **hourglass** symbol indicates the AIX HMP/6000 is busy processing the operation.
3. A **circle bisected with a diagonal line** indicates an error condition.

13.5.2 Common Window Attributes

The following *buttons* and their associated operations are common to most AIX HMP/6000 windows and forms:

Apply

The Apply operation transmits and accepts SNMP parameter information contained in the form, to/from the management module agent.

The data entered into a form has no effect on the agent until this button is activated. Once activated, you will receive a message confirming the transmission of data to the agent.

Quit

The Quit operation exits a form without transmitting the information in the form to the agent. Quit does not undo changes transmitted by previous applications of the Apply operation.

Net Get

AIX HMP/6000 obtains information about the hub it is managing by polling the master management module. In order to reduce network traffic, AIX HMP/6000 does not poll for information that is currently held in memory when the program opens a form. When the information held in memory is used, the following message is displayed, **Data located in memory**.

If you believe the information may not be current, click on the Net Get (or Network Get) operation to force the polling of the master management module to retrieve the current data. If the retrieve was successful, the message **Retrieve was successful** will be displayed in the Information Area of the form.

Confirming a Change

If you invoke a command that may disrupt the system, such as a module reset or exiting a hub for example, AIX HMP/6000 will automatically invoke a **Hub Confirmation** form.

The **OK** operation confirms a change and continues the operation and the **Cancel** operation returns you to AIX HMP/6000 without performing the requested operation.

Note that in some panels such as the Browser selection, the *ok* button will terminate a function.

13.6 Installation Experiences

Using the AIX *System Management Interface Tool (SMIT)* installation of AIX HMP/6000 is very simple. This section lists the prerequisites required for the installation and describes the steps that you will need to follow to install AIX HMP/6000 using SMIT.

If you are not familiar with SMIT, additional information is available in the *AIX General Concepts and Procedures for IBM RISC System/6000*; however, we have attempted to describe the steps in sufficient detail for the novice user.

13.6.1 Prerequisites

This section lists the recommended hardware and software requirements for the installation and operation of AIX HMP/6000.

13.6.1.1 Hardware Prerequisites

If you are *installing* AIX HMP/6000 from a preloaded system you will require a tape drive which is compatible with the media on which you have received your software. This will be either an 8 mm or 1/4-inch cartridge tape drive.

13.6.1.2 Software Prerequisites

AIX HMP/6000 requires the following software:

- AIX Version 3.2 (or later)
- AIX NetView/6000 Version 1 (not Version 2 at the time of writing)
- AIXWindows Environment/6000 Version 1.2 (or later)
- TCP/IP (an optional component of AIX)

13.6.1.3 A Minimum Recommended Workstation Configuration

- An IBM RISC System/6000 with a mouse and color graphics adapter (4-bit plane minimum)
- 32MB RAM
- 96MB paging space
- 30MB disk space (depending on the configuration and the size of the managed network, additional disk space may be required for log files)
- A color monitor (typically larger is better as often it is convenient to display multiple windows simultaneously)
- An appropriate network interface

13.6.2 Installation of AIX HMP/6000

Before you begin:

You must be logged in as root (super user) to perform the installation.

You must use an AIX operating system shell. The installation process invokes shell scripts that require this.

Remember that AIX is case sensitive.

13.6.2.1 Installation Tasks

1. Insert your IBM AIX HMP/6000 installation tape (8 mm or 1/4-inch) into the tape drive. If the tape drive is set with the default options, this will allow tape retension while you continue with the following tasks. It is both normal and common for tape drives to be configured with the retension option set to yes.

   If you are setting up a new machine, more than likely it will be **preloaded** with the software that was ordered with the machine. Note that *preloaded* software images still need to be *installed*. Preloaded software can be installed directly from disk which is much faster than tape or diskette. Obviously in this scenario, you do not need to worry about the software tape/diskette.

2. To access the installation menu, type the following at the AIX command line. Normally the root signon command prompt is designated by the **#** symbol.

   ```
   smit
   ```

   This will cause the main AIX *System Management* menu to be displayed.

   If AIXWindows is running then SMIT will be displayed in a Motif graphical format and you will be able to use your mouse to make the selections. If you invoke SMIT from an asynchronously attached terminal or from a graphics terminal without AIXWindows running, then you will invoke an ASCII SMIT application and you will need to use the keyboard *arrow* keys to move about the application.

3. Select **Installation & Maintenance** from the System Management menu.

4. Select **Standard Installation & Maintenance** from the Installation & Maintenance menu.

5. Select **Software Installation & Maintenance** from the Standard Installation & Maintenance menu.

6. Select **Install/Update Software** from the Software Installation & Maintenance menu.

7. Select **Install Software Without Updates** from the Install/Update Software menu.

   Note, at the time of writing, this installation process was tested using the original release of AIX HMP/6000 known as General Release or GA code. The installation tape that we used contained no updates. This may not be the case for future releases of the software. Obviously, if you are installing from a tape that contains updates that you wish to install, choose the *Install Software With Updates* option. There is an option under the *Software Installation and Maintenance* menu to list the products on the media from which you are installing.

8. Select the input device you wish to install from.

   If you are running a Motif (graphical) SMIT application, simply click on the *list* button to display a list of valid device selections from which you can choose.

   If you are running an ASCII SMIT application, you can display a list of valid device selections by highlighting the input field with the cursor and pressing the *F4* key. Use the cursor to select the appropriate device.

If you are installing AIX HMP/6000 from a preloaded RISC System/6000, then your device will be the */usr/sys/inst.images* which is the default preload directory.

9. Select software to install.

   The *Install Software Without Updates* dialog menu will prompt you for the software you wish to install.

   Again a list of valid options can be displayed by clicking on the list button or pressing the F4 key, depending on how you invoked SMIT.

   The AIX HMP/6000 product documentation says that if you are installing without updates you can manually enter *hmp6000.base.all* in this input field even if the option is not present in the input list. This was not tested in our installation.

10. Use the default options for the remaining fields and run the command.

    With the default options accepted for the remaining fields, the GA code with no updates on 8 mm media took approximately 5-10 minutes to install.

Chapter 14. Ethernet Management Functions

This chapter will look at Ethernet management functions for the IBM 8250 Multiprotocol Intelligent Hub. The differences between *in-band* and *out-of-band* management of the Ethernet management module will be highlighted.

While the examples in this chapter are documented in reasonable completeness, it assumed that the reader has a fundamental understanding of how to use both AIX HMP/6000 and the 8250 console terminal.

It is not the aim of this chapter to document every possible command for every Ethernet module. Complete command reference material can be found in the documentation supplied with your modules.

This chapter will address the following sections:

- Configuration
- Non SNMP Agent Module Management
- Statistics Gathering
- Access and Security

If you have not already done so, you may benefit from familiarizing yourself with the material covered in Chapter 12, " Hub Management - Before You Start" on page 275 before you progress any further.

14.1 Configuration

This section will look at the configuration management options for the 8250 Ethernet modules.

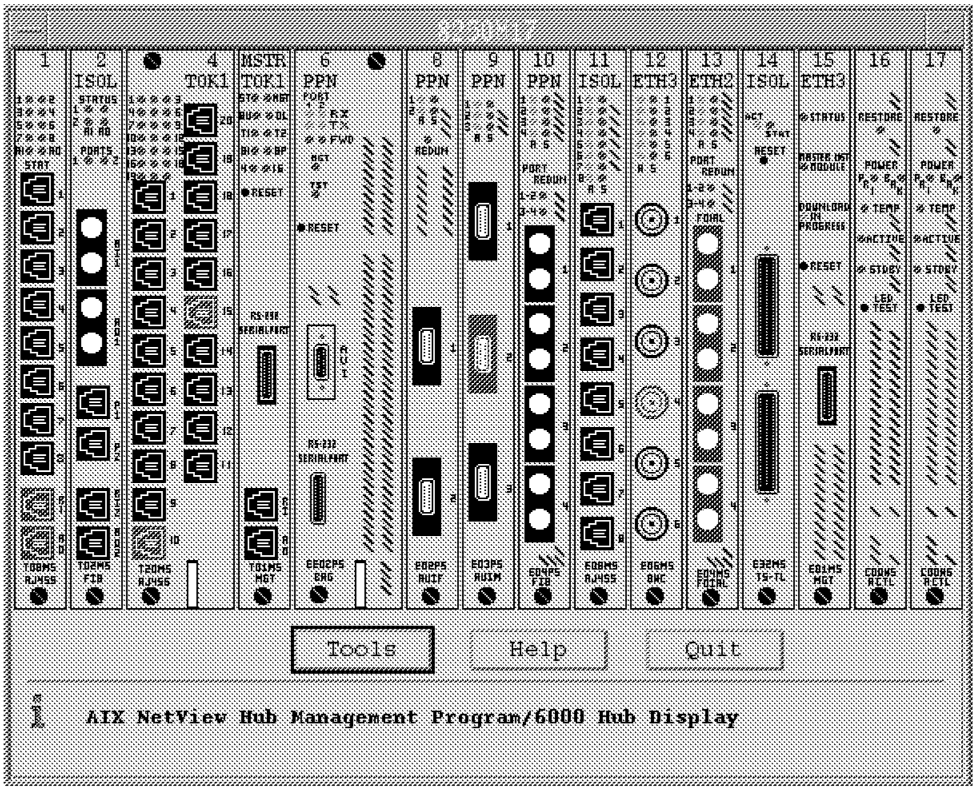
Table 56 (Page 1 of 2). Ethernet Modules

Ethernet Modules	IBM Model Numbers	AIX HMP/6000 Identifiers
Ethernet Management	3819EM	E04MS-MGT
Ethernet Fiber	3805EF, 3806EF, 3807EF 3808EF, 3809EF, 3810EF 3811EF, 3812EF, 3813EF	E04MS-FIB E04PS-FIB E02PS-FIB
Ethernet FOIRL	3814EFL, 3815EFL, 3816EFL	E04MS-FOIRL
Ethernet 10BASE-T	3800E 3801E 3802E	E08MS-RJ45S E12MS-TELCO E12PS-TELCO
Ethernet Transceiver	8303ET	E03PS-AUIM
Ethernet Repeater	3804ER	E02PS-AUIF
Ethernet BNC	3817EF	E06MS-BNC

Table 56 (Page 2 of 2). Ethernet Modules		
Ethernet Modules	**IBM Model Numbers**	**AIX HMP/6000 Identifiers**
Ethernet Terminal Server	3818ES, 3896ES	E32MS-TS-T, E32MS-TS-TL
Ethernet Bridge	3828EB	EE02PS-BRG

Remember that *in-band* management uses the SNMP and associated commands while *out-of-band* management includes only those commands entered from a direct RS-232 attached terminal console or pseudo-attached equivalent (a Telnet session for example).

For reference purposes we have reproduced the AIX Hub Display windows for each of the 8250s in our network; see Figure 151 and Figure 152 on page 305.



AIX NetView Hub Management Program/6000 Hub Display

Figure 151. The AIX HMP/6000 Hub Display Window. The Hub Display window for the 8250 Model 17.

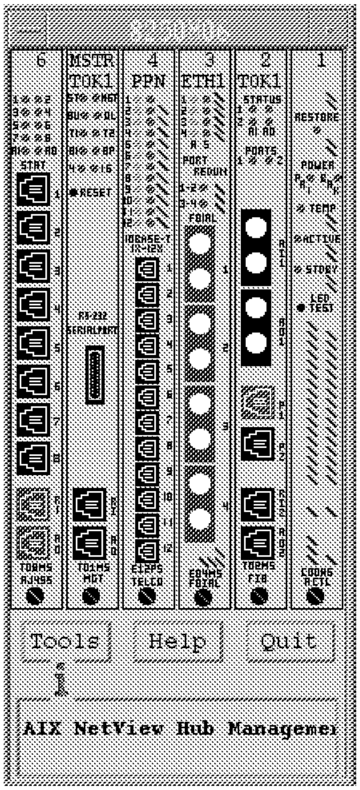


Figure 152. The AIX HMP/6000 Hub Display Window. The Hub Display window for the 8250 Model 6.

14.1.1 Ethernet Management Module: In-band Management

From the Hub Display window shown in Figure 151 on page 304, click the mouse anywhere on the Ethernet management module in slot 15, except the RS-232 port, to display the main menu of management options for this module.

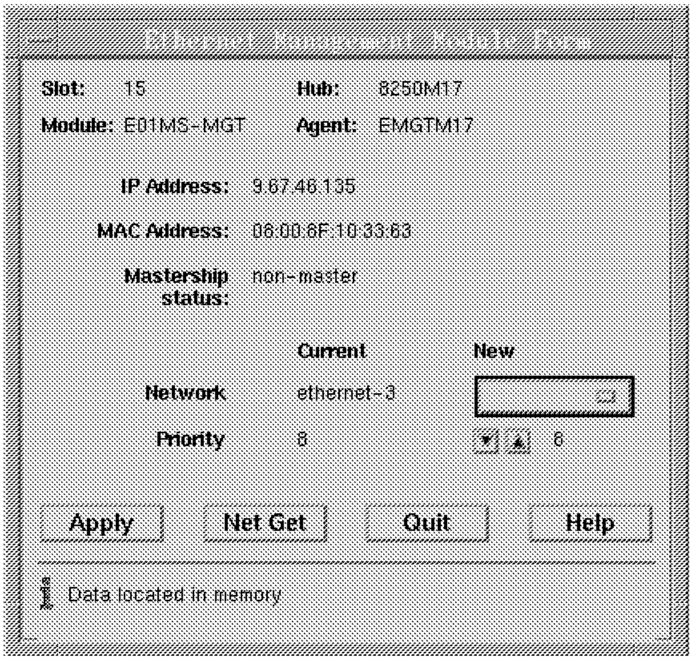
The Ethernet **Management Module Menu** has the following options:

- Configuration
- Information
- Echo
- Ping
- Login
- Reset Module
- Download
- Help

Each of these are described in more detail below.

14.1.1.1 Configuration

Selecting the *Configuration* option displays the **Ethernet Management Module Form**; see Figure 153. This form allows you to configure the network to which the module is connected and the mastership priority of the module.



Ethernet Management Module Form

Slot: 15 Hub: 8250M17

Module: E01MS-MGT Agent: EMGTM17

IP Address: 9.67.46.135

MAC Address: 08:00:8F:10:33:63

Mastership status: non-master

	Current	New
Network	ethernet-3	
Priority	8	8

Data located in memory

Figure 153. The Ethernet Management Module Form. This is main configuration form for the Ethernet management module.

To configure the **network** to which the module is attached, click the mouse once on the *new* button in the form. This will display a selection list of valid options from which you can choose.

The list of available network options is determined by the configuration of the remainder of the hub.

Refer to 6.2, “Advanced Backplane Architecture” on page 109 for a detailed explanation of the IBM 8250 Multiprotocol Intelligent Hub backplane architecture which dictates the allowable network mix on the hub.

The *up-arrow* and *down-arrow* buttons allow you to increase and decrease the **mastership priority** of the Ethernet management module. This parameter is used by the mastership election process to determine which module becomes the hub master when there are multiple management modules (Ethernet and/or token-ring) in the same hub.

A mastership election may be invoked for a number of reasons, such as the execution of the *reset mastership* command, a *power failure* in the hub, execution of the *reset concentrator* command or *failure of the current master*.

The highest priority is 10 decreasing to the lowest, 1. The election process is most efficient if the intended master has a priority of 10 and all other management modules have a lower priority.

If more than one management module has a priority of 10 then the results of a mastership election are unpredictable. The first to complete initialization will become the master and the remaining management modules will be slaves.

In addition to the *warnings* highlighted below you should think carefully about the implications of your management module priority settings.

Consider the implications of a scenario where the intended slave management modules have a configuration different from the intended master module and the master fails.

For example, say we have two management modules each with different configuration parameter settings in their non-volatile memory from a previous *save* command. If you assign both the intended master and the intended slave the same priority, then after the power-on, the intended slave may become the master which will result in the 8250 being configured in a way other than was planned and expected.

This is only a single example, of which there are many, so care must be exercised in assigning mastership priority to the management modules.

WARNING

At this level of microcode a mastership election will result in an Ethernet management module becoming the master ahead of a token-ring management module regardless of the mastership priorities set in each module, given the following conditions:

- The token-ring management module has *diagnostics enabled* **and**
- The mastership election was *not* invoked by the reset mastership command **and**
- The token-ring management module is at microcode level 1.10 -B **and**
- The Ethernet management module is at microcode level 3.1 -A

The reason for this is the longer time the token-ring management module requires to run diagnostics during startup versus the initialization time of the Ethernet management module. That is, the Ethernet management module is wrongly allowed to assume mastership because the token-ring management module has not had sufficient time to establish itself as a mastership contender.

The *reset mastership* command does not cause the token-ring management module to reboot, (and hence run diagnostics), therefore, it does not cause this anomaly.

Note that the token-ring management module factory default enables diagnostics.

To fix this problem, ensure that the token-ring management module has a higher mastership priority than the Ethernet management module, and execute the following commands at the token-ring management module console:

```
set device diagnostics disable

reset mastership
```

WARNING

At this level of microcode, if the Ethernet management module is allowed to become the master, a token-ring management module will not be recognizable by the Ethernet management module.

- The token-ring management module is at microcode level 1.10 -B.
- The Ethernet management module is at microcode level 3.1 -A.

Normally, where a token-ring management module and Ethernet management module are to coexist in the same 8250, the token-ring management module must be configured as the master to ensure the full availability of the token-ring management functions, (such as beacon recovery).

However, as stated in the above warning, we found that a master Ethernet management module actually renders the token-ring management module useless. The token-ring management module becomes isolated from the backplane though this is *not* reflected by the `show module` command. In fact, a master Ethernet management module will display the module as *N/A* in the output of the `show module all` command for the token-ring management module.

Therefore you must ensure that the token-ring management module is always the master. This can be done using the following:

1. Ensure that the token-ring management module has a greater mastership priority than the Ethernet management module. To change the token-ring management module mastership parameter you must have the console attached directly to the token-ring management module. This is because, the Ethernet management module is unable to recognize the token-ring management module.
2. Issue the `reset mastership` command from the master management module (Ethernet management module) and allow the token-ring management module to become the master and the Ethernet management module the slave.

   The token-ring management module will become the master and will learn the configuration of the 8250 and all the installed modules by polling them. This means that there will be no need to reconfigure the network parameters.

All other parameters in the *Ethernet Management Module Form* are read-only. You should especially note that you cannot configure parameters such as the agent IP address for the Ethernet management module via AIX HMP/6000.

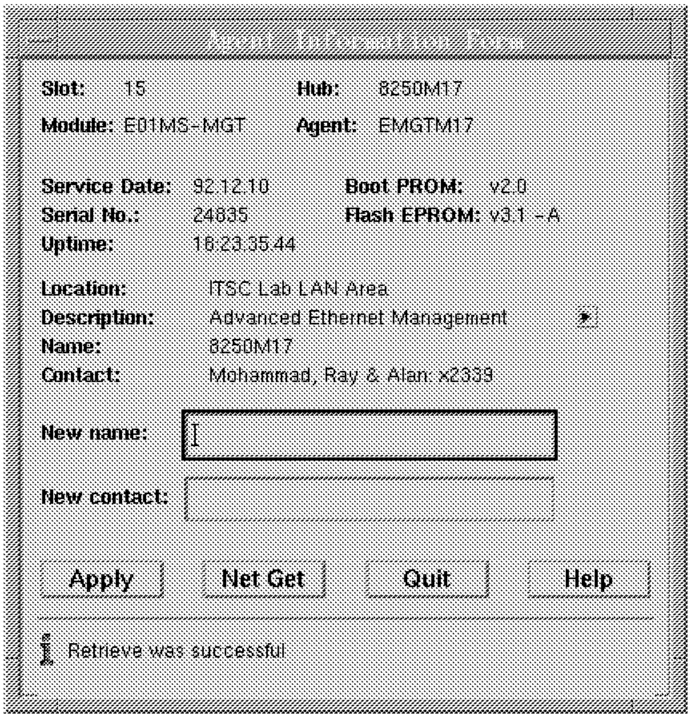
This means that the setup required for the establishment of IP connectivity between the SNMP network manager and the Ethernet management module must be accomplished (at least in part) with a direct attached asynchronous ASCII terminal.

See Chapter 12, “ Hub Management - Before You Start” on page 275 for more information on initial setup requirements.

14.1.1.2 Information

Additional information about the Ethernet management module can be displayed by clicking the left mouse button on the *Information* option.

Again this form, see Figure 154, provides mostly read-only information.



Agent Information Form

Slot:	15	**Hub:**	8250M17
Module:	E01MS-MGT	**Agent:**	EMGTM17
Service Date:	92.12.10	**Boot PROM:**	v2.0
Serial No.:	24835	**Flash EPROM:**	v3.1 -A
Uptime:	18:23:35.44		
Location:	ITSC Lab LAN Area		
Description:	Advanced Ethernet Management		
Name:	8250M17		
Contact:	Mohammad, Ray & Alan: x2339		
New name:			
New contact:			

Retrieve was successful

Figure 154. The Ethernet Agent Information Form. This is primarily an information form for the Ethernet management module.

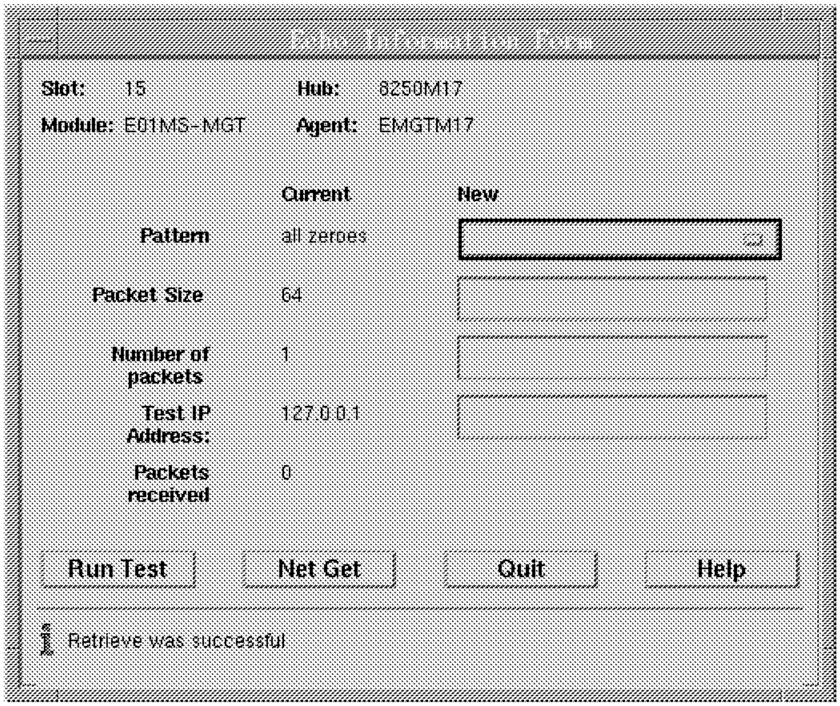
The agent *name* and *contact* information may be altered from this form by clicking the left mouse button in the corresponding input field for each parameter and entering the desired change.

These fields correspond to the standard MIB-II variables **sysName** and **sysContact**.

The information in both the Configuration form and the Information form can also be viewed via the *MIB Browser* under the *Tools* menu of *AIX NetView/6000*. In fact, this tool can be used to alter the *Location* field in the Information form as it corresponds to the **sysLocation** variable in the standard mib-2 database and this tool has write permission to it. All other fields are, however, read-only MIB variables so they can only be viewed.

14.1.1.3 Echo

Clicking on the **Echo** option displays the **Echo Information Form** shown in Figure 155 on page 310.



Echo Information Form

Slot: 15 Hub: 8250M17

Module: E01MS-MGT Agent: EMGTM17

	Current	New
Pattern	all zeroes	
Packet Size	64	
Number of packets	1	
Test IP Address:	127.0.0.1	
Packets received	0	

Retrieve was successful

Figure 155. The Echo Information Form

This form enables the network administrator to send ICMP echo requests from the Ethernet management module agent to other IP addresses on the network. An ICMP echo request is commonly referred to by its generic command name, *ping*.

The Echo Information Form also allows the administrator to set some of the parameters associated with the ICMP echo command.

The bit pattern sent in the ICMP packet can be specified by setting the **Pattern** parameter. Possible combinations are all zeros, all ones or mixed. Setting this pattern may be useful if you have the IBM Trace program (or equivalent) available to analyze your network.

You can also set the **Packet Size** parameter. The packet size must be between 64 and 1500 bytes in length.

Unlike the AIX HMP/6000 Ping form described in the next section, the echo form does allow you to set the number of ICMP packets to be transmitted during the test.

14.1.1.4 Ping

Clicking on this option tests IP connectivity between the management station running AIX HMP/6000 and the selected Ethernet management module.

This test is, however, somewhat limited as only one ICMP packet is sent. If this packet is lost then the test fails. For a marginally better test you may consider pinging the Ethernet management module from either AIX NetView/6000 or the AIX command line as this will attempt to send ICMP packets in succession until explicitly stopped, thus providing a more accurate result.

14.1.1.5 Login

At the time of writing, the AIX HMP/6000 *Login* feature for the Ethernet management module was not available. This is because the Ethernet modules implement the remote login feature via a proprietary protocol called RCP (Remote Character Protocol) which uses the IEEE 802.2 link control layer. This protocol is not implemented by the AIX operating system nor do the Ethernet modules implement Telnet or rlogin. Therefore, the only way to do a remote login to an Ethernet module is via another Ethernet module or the Ethernet bridge module which are the only two 8250 modules which have implemented this protocol. The following few paragraphs provide some brief information about RCP.

The Ethernet remote login feature is somewhat limited because the RCP protocol is implemented only at the link layer which means it is not routable. This means that remote login sessions with Ethernet modules cannot be supported across IP routers.

The RCP protocol defines a master/slave relationship between the device initiating the login session and the device supporting the session respectively. Terminal characters are sent separately between the master and the slave. On completion of the command, the slave sends the output of the executed command.

RCP also monitors the session to determine if the session is still active. Basically the master pings the slave once every 60 seconds and should the slave fail to respond within the timeout period, the session is aborted.

You should not confuse the remote_login command with the UNIX *rlogin* command; they are different.

14.1.1.6 Reset Module

Clicking on this option is equivalent to executing the command for the Ethernet management module:

```
reset module 15
```

As described in the commands reference supplied with the Ethernet management module, this command is normally only invoked when the module is not functioning as expected.

Be aware that invoking this command will generate approximately 24 error windows to AIX HMP/6000 instructing that hub rediscovery may be necessary.

14.1.1.7 Download

This facility allows you to download new levels of software onto the Ethernet management module. Unfortunately, we did not have Ethernet code readily available to test the Ethernet management module download feature. Due to this, the following is based on our experiences with the token-ring management module download process.

Display the **Download Form** by clicking on this option from the *Management Module Menu*. This form allows you to set the parameters required to download new microcode to the Ethernet management module.

The documentation for the in-band download command supplied with the Ethernet management module indicates that the TFTP (Trivial File Transfer

Protocol) parameters must be explicitly set using the `set tftp` command before you can execute an in-band download.

This is not the case when an in-band download is initiated from AIX HMP/6000. This is because the download form provides input fields for the TFTP parameters which renders this requirement superfluous.

The in-band download procedure is as follows:

1. Make an AIX directory to store the image to be downloaded. This is arbitrary; you can use whatever directory you wish.

   ```
   cd /usr/etc/hmp
   ```

   ```
   mkdir download
   ```

2. Copy the download image from the diskette to the /usr/etc/hmp/download directory that you created in step 1. Note that the diskette is formatted for DOS or OS/2 so you will need to use the AIX `dosread` command.

   If required, the DOS `dir` command can be used to read the contents of the diskette.

   To read the file into the AIX file system, change to the target directory and copy the file:

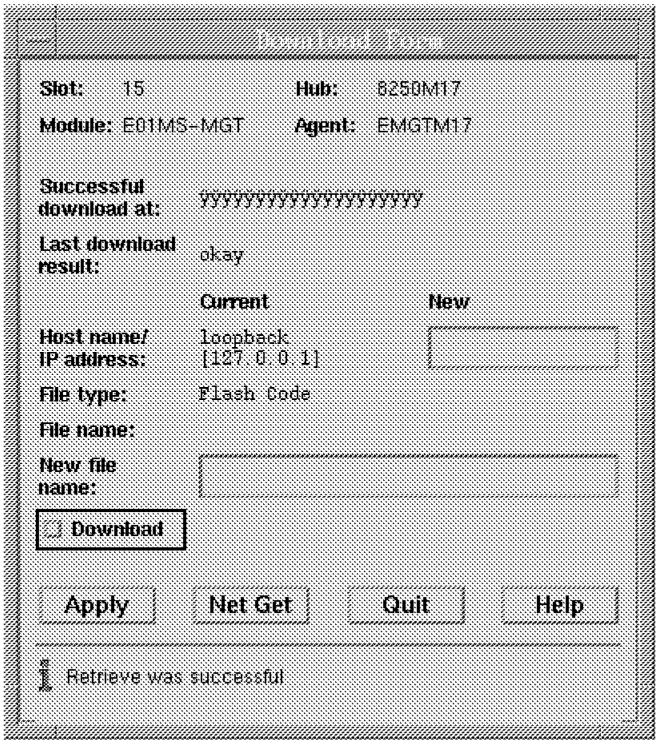
   ```
   cd /usr/etc/hmp/download
   ```

   ```
   dosread emm31b emm31b
   ```

   The dosread command parameter syntax is *source* then *destination* so the effect of this command will be to create a file image of the same name. This is arbitrary if you wish to rename it.

   If you have not already done so, invoke the *download* form from the Ethernet management module menu.

   The form will look similar to the one shown in Figure 156 on page 313.


Download Form

Slot: 15 Hub: 8250M17

Module: E01MS-MGT Agent: EMGTM17

Successful download at: yyyyyyyyyyyyyyyyyyyy

Last download result: okay

	Current	New
Host name/ IP address:	loopback [127.0.0.1]	
File type:	Flash Code	
File name:		
New file name:		

Retrieve was successful

Figure 156. The Download Form

3. Set the download form parameters.

   Set the **Host name/IP address** parameter to the IP address of your RISC System/6000 which you wish to download from.

   The **File type** is set to *flash code* and cannot be modified for the Ethernet management module.

   Set the **File name** of the AIX file which you wish to download. This should (obviously) be consistent with the file name you created in step 2.

4. Activate the Download button.

   The *Download* button is merely a safety check that forces you to explicitly confirm that you wish to perform the download with the current parameter settings.

   Clicking on the Download button will not initiate the download. The button will turn dark gray when active.

5. Initiate the download.

   To start the download process click on the *Apply* button.

   If you did not activate the Download button (see previous step) this will simply send an SNMP *set* command to the Ethernet management module agent to change the current values corresponding to the parameters in the form.

During the download you will lose connectivity with the agent. This is indicated by a message in the Hub Display window. When the download is complete a message indicating that connectivity has been re-established, will also be displayed.

If you attempt to perform a *Net Get* from the form during the download you will also get an error message indicating a timeout error. These errors are nothing to be concerned about.

A Caution

Although we did not experience the following problem with the in-band download procedure, it has been reported by other people. So, it is mentioned here just in case it is encountered by the reader.

There is a MIB variable called **tftpStart** which dictates whether or not, and in what direction, the TFTP file transfer will execute. This variable is of type **integer** and supports the following values:

- **tftpNoTransfer**

  Do not perform a transfer.

- **tftpGet (2):**

  Transfer to the agent - download.

- **tftpPut (3):**

  Transfer to the server - upload.

To perform a download the *tftpStart* variable must, obviously, be set to 2.

Sometimes it is required that this variable be explicitly set before attempting the download. Unfortunately, at the time of writing, the cause of this anomaly was unknown.

There are two ways of setting this variable. It can be altered using the AIX NetView/6000 *Browser* tool or it can be set by issuing the following SNMP command:

```
snmpset node community .1.3.6.1.4.1.49.2.6.1.0 integer 2
```

The *node* parameter should be the name or IP address of your agent and the *community* parameter should be valid for that same agent. The dotted decimal parameter is the MIB identifier for the *tftpStart* variable.

14.1.1.8 Help

Clicking on this option invokes the AIX HMP/6000 context sensitive help facility for the Ethernet management module

14.1.2 Ethernet Management Module - Out-of-Band Management

You can use an ASCII terminal, attached directly or via a communications line to the RS-232 port on the Ethernet management module, to access the management functions provided by the Ethernet management module.

To use the ASCII terminal, the terminal should be set up as described in 12.2, “Console Configuration” on page 279.

Once connected, you can log in from the terminal to the Ethernet management module as an *administrator* or a *user* using the appropriate password. For more information about passwords, refer to 14.4, “Access and Security” on page 339.

If the Ethernet management module is a *slave*, you can collect statistical information about the network that the Ethernet management module is attached to. Also, you will be able to issue configuration commands that affect the slave Ethernet management module itself. However, you can not issue configuration commands about the other modules installed on the 8250, nor would you be able to receive fault information about the 8250 and the installed modules.

A master Ethernet management module will allow you to configure all the installed modules, as well as allow you to collect statistical information about the network to which the Ethernet management module is connected.

A master management module can be used to control and monitor a slave Ethernet management module slave by using the following commands:

- Reset module
- Set module
- Show module

Some commands, however, require that you be specifically logged into the Ethernet management module console. As an example, you cannot change the IP address of a slave management module via the terminal attached to the master management module. In cases like this, using the remote-login command can be of great use in controlling multiple Ethernet management modules from a single terminal.

A description of the commands supported by the Ethernet management module is provided below. For complete command information, refer to the documentation provided with your Ethernet management module.

14.1.2.1 Ethernet Management Module Commands List

The following out-of-band commands are executable by the administrator from the Ethernet management module console:

- **boot:**

  Used to return from maintenance mode and to boot the operational code in the flash EPROM. This command is only available from maintenance mode.

- **clear:**

  Used to reset or clear the following configuration variables:

  community:

  Deletes an entry in the community table.

  counter:

  Clears the statistical counters.

  error_log:

  Erases the error log.

  security port:

  Enables you to set a port′s MAC address to zero and to disable security.

  This command is only available for the advanced Ethernet management module.

tftp result:

Clears the TFTP result from the *show tftp* command display. This should be used before you begin an in-band download.

This command is only available for the advanced Ethernet management module.

- **download:**

  Performs both *in-band* and *out-of-band* loading of new Ethernet management module software.

  In-band download is available in both maintenance and normal mode.

  Out-of-band download is available *only* in maintenance mode.

- **logout:**

  Terminates the current logon session.

  If you are logged into a remote Ethernet management module or an Ethernet bridge module, this command will terminate the connection to the remote device and will re-establish a connection with the local Ethernet management module.

  If the connection is via a modem and the *hangup* parameter is *enabled* then the logout command also disconnects the modem.

- **maintain:**

  Enters maintenance mode.

- **monitor:**

  Allows you to view (monitor) ongoing performance statistics based on a selectable polling period.

- **ping:**

  Used to test connectivity between the Ethernet management module and another IP addressable device on the network.

- **remote_login:**

  Allows you to log in remotely to another Ethernet management module or an Ethernet bridge module. This will provide you with an out-of-band management session on the remote device.

  You can only log in remotely one level down. That is, if you remotely log in to a device and you wish to remotely log in to another, you must log out of the first device before attempting to log in to the second.

- **reset:**

  This command allows you to refresh or reassign the following:

  concentrator:

  Allows you to reboot both the hardware and the software (cold boot) of the 8250 hub.

  Diagnostics will be executed for those modules which have the *diagnostics* parameter enabled.

  Note that you must save or revert any unsaved changes before this command will execute.

  device:

Resets the Ethernet management module to which you are logged into.

Note that you must save or revert any unsaved changes before this command will execute.

mastership:

Will force a mastership re-election in hub.

module:

Will perform a hardware reset of the module. This command should only be used if a module is not functioning correctly.

You cannot reset the controller module using this command, you must use the *reset concentrator* to do this.

You cannot reset the Ethernet management module to which you are logged on to; you must use the *reset device* command to do this.

power_supply:

Used in a situation where the hub is working off the backup power supply. This command will switch from the primary to the secondary power supply.

Note that you must save or revert any unsaved changes before this command will execute.

A power supply switch performs a warm boot which causes the hub and all the modules to reset.

- **revert:**

  Use this command to return the configuration to the settings that were in effect as of the last save. It is possible to revert selected parameters; however, *revert security* and *revert tftp* options are only available for the advanced Ethernet management module.

- **save:**

  Saves the current configuration values established by the *set* command. It is possible to save selected parameters; however, *save security* and *save tftp* options are only available for the advanced Ethernet management module.

  Only *saved* values are effective upon a reset.

- **set:**

  Enables you to change configuration values. Following is a list of available parameters:

  alert:

  Allows you to enable or disable the notification of an alert (trap) type to an SNMP management station such as AIX NetView/6000.

  The following three alert types are valid:

  1. **authentication:**

     This trap is issued when an SNMP request is received from a network manager whose IP address or community name is not valid for the attempted operation.

  2. **change:**

     Issued when any configuration change is made to this hub.

3. **hello:**

   Issued when an existing Ethernet management module is reset. This trap is sent once every minute until a valid SNMP PDU (Protocol Data Unit) is received or for up to 4 hours and 15 minutes, at which time it stops sending the alert.

clock:

Sets the time clock.

community:

Creates entries in the community table for network management stations that will issue SNMP requests to, or receive traps from, this Ethernet management module.

concentrator platform:

Use this command to inform the Ethernet management module as to the type of hub platform in which it is installed.

The default setting is the 8250 Model 17. If you do not reset this parameter for the 8250 Model 6, AIX HMP/6000 will depict it as a a Model 17.

device:

Allows you to configure the parameters listed below:

> **contact:**
>
> A textual string describing the person responsible for the module/hub.
>
> **default_gateway:**
>
> Is used to set the IP address of the gateway that should be used when the Ethernet management module wants to send TCP/IP packets to an address which is not on the local network.
>
> This parameter is useful when sending traps to a management station on a different network. It is possible to configure a separate gateway address for each of the three possible Ethernet networks on the backplane.
>
> **diagnostics:**
>
> Enables or disables diagnostics during the boot of the Ethernet management module.
>
> **dip_configuration:**
>
> Allows the module to boot according to either the settings of the hardware dip switches or the software settings (management module settings).
>
> **ip_address:**
>
> Use this parameter to set the Ethernet management module′s IP address. A unique IP address can be configured for each Ethernet network on the backplane to which the management module may attach.
>
> **Location:**
>
> A textual string describing the location of the module/hub.

name:

A symbolic name that may be used instead of the IP address.

password:

Establishes a security password for an administrator and/or user. The administrator will have access to *all* the commands.

subnet_mask:

Used to specify the subnetwork mask that is to be used for local subnetting. Refer to 4.2, "IP Addressing" on page 74 for an explanation of subnetting.

You can configure a unique subnet mask for each Ethernet network on the backplane to which the management module may attach.

trap_receive:

Use this command to enable this Ethernet management module as a trap receiver for other SNMP devices on the network. Note that, an Ethernet management module will not perform any further forwarding of the traps received.

This feature is only available for the advanced Ethernet management module

download network:

Specifies the Ethernet network on which the in-band download will occur. This command is saved automatically once you press *Enter*.

This feature is only available for the advanced Ethernet management module.

module:

Enables you to configure the following module parameters:

cable impedance:

Used to set the cable impedance level for the token-ring module lobe ports.

You specify 100 ohms for Unshielded Twisted Pair and 150 ohms for Shielded Twisted Pair.

crossover:

Enables/disables crossover mode for port 8 of the 10BASE-T module. When connecting two 10BASE-T modules one port must be crossed and the other uncrossed; otherwise, an external crossover cable will be required.

fifo_fill_level:

Controls the number of bits loaded into the internal FIFO buffer before the bits are unloaded.

This command is only applicable on certain older twisted pair products that have FIFO capability.

low_light_warning:

When enabled the low light warning LED will indicate (6 blinks) that a weak light signal is being received from an Ethernet fiber module.

mastership priority:

Sets the priority level for the management module. This will be used in the event of a mastership election.

module_bypass:

Use this command to insert token-ring MAU modules into a ring to which the RI and RO ports of the MAU are connected. When set to *bypass*, ring traffic still passes through the RI/RO ports on the MAU module but not its eight lobe ports. This is automatically set to bypass mode when the MAU is placed in a hub where there is an operational management module.

network:

Assigns the module to a particular network.

ring_speed:

Enables you to set the module to operate at a transmission rate of either 4 Mbps or 16 Mbps for token-ring networks.

port:

Allows you to configure the following port specific parameters:

collision:

The collision mode may need to be set to *alternate* if used with non-IEEE 802.3 devices. *Normal* mode is used for IEEE 802.3 devices.

half_step:

Enables half-step signalling for ports on the transceiver module. Half-step enabled is the default setting and is used for IEEE 802.3 and Ethernet Version 2.0 devices. Early Ethernet and non-802.3 devices may require full-step signalling.

high_power:

Enables or disables the port from receiving or transmitting at high power. This command pertains to the port switching fiber modules only.

link_integrity:

The 10BASE-T standard requires that link integrity be enabled. Some older non-10BASE-T equipment may require that you disable link integrity on the port.

This parameter must be set to the same value at both ends of the link.

low_light_warning:

When enabled the port will indicate that the light level received is weak.

This command pertains only to the port switching fiber modules.

mode enable/disable:

Use this command to explicitly enable or disable a port.

In a hub where a management module is active, all ports of newly installed media modules are automatically disabled for security purposes.

mode local/remote:

This command allows you to configure the port access for the Ethernet terminal server module. Set this parameter to *remote* if the port will be accessed from a remote device using a modem connection. The default setting is *local*.

mode redundant/non_redundant:

Establishes redundancy between two ports. One port is established as the primary link and the second as a backup. In the event of the primary link failure, the backup link will take over.

When operating with an advanced Ethernet management module, port redundancy can be set across modules.

Care needs to be taken when configuring port redundancy, so that the backup configuration does not cause a network loop. The Ethernet management module command documentation details those situations which require care.

mode remote_diagnostics/non_remote_diagnostics:

Use this command to establish the *remote diagnostics* protocol on a pair of 10BASE-T ports. This protocol enables the module to work dynamically with an IBM Fault Tolerant 10BASE-T Transceiver to sense problems and switch automatically to a backup link.

Note that you must have link integrity enabled on the transceiver for this command to work correctly. It will automatically be enabled on the module when you enable remote diagnostics.

This feature currently only works on the Ethernet 50-pin module.

mode remote_failure_signalling:

Establishes remote failure signalling on redundant FOIRL links.

network:

Assigns the port to a specific network.

receive_jabber:

Can be enabled for the Ethernet 50-pin module. When enabled, if a jabber condition occurs and the transceiver or repeater device fails to halt it, the Ethernet management module will protect the network by disconnecting the link after 10 msecs.

The default setting is disabled to conform with the 10BASE-T standard.

sqe_test:

Enables or disables the SQE test for ports on the Ethernet transceiver module. The SQE test normally needs to be disabled to allow this port to connect to either a repeater or multiport transceiver.

squelch:

May be set to either *normal* or *low*. It is factory set to normal to comply with the 10BASE-T standard.

A low squelch level will sense a weaker signal allowing a longer link distance. However, this increases the risk of losing packets due to impulse noise.

type:

Used to define FDDI ports as either master or slave ports. Normally used for redundant configurations.

security:

Enables the configuration of the following security parameters:

port mac_address:

Used to define address to port security on individual ports. When a MAC address is set for a specific port and the security is enabled (see 14.1.2.1, “Ethernet Management Module Commands List” on page 315), and the Ethernet management module detects a change in a port′s source MAC address, it will send an alarm to the Ethernet management module console or a trap to an SNMP network management station, and shut down the port. Multiple MAC addresses may be assigned to the same port.

This command is only available for the advanced Ethernet management module.

port mode:

Enables security for a port which has been assigned a MAC address(es) using the *set security port mac_address* command.

terminal:

Enables the configuration of the following parameters for the terminal attached to the RS-232 port on the Ethernet management module:

baud:

Sets the transmission rate of the Ethernet management module RS-232 port.

data_bits:

Sets the number of data bits used in the transmission.

hangup:

Used to automatically disconnect a modem attached to the RS-232 port when you log out.

parity:

Establishes the parity setting to be used during the transmission.

prompt:

Allows you to customize the prompt you receive at your Ethernet management module console.

stop_bits:

Establishes the number of stop bits to be used during the transmission.

timeout:

Will automatically log out the user after a period of inactivity.

If hangup is also enabled and the terminal is modem attached, the modem will also be disconnected after the timeout.

tftp:

Enables the configuration of the following parameters which are used for in-band downloads.

This command is only available for the advanced Ethernet management module:

file_name:

Sets the name of the file on the file server to be downloaded.

server_ip_address:

Sets the IP address of the server host which contains the file to be downloaded.

trunk:

The following trunk parameters can be configured using this command:

ring_in/ring_out cable monitor:

Enables or disables cable monitor mode on the copper RI and RO ports for token-ring modules. If enabled and a cable fault is sensed, the RI and RO ports will *wrap* to keep the ring operational.

ring_in/ring_out mode:

Enables or disables the RI and RO ports on token-ring modules.

ring_in network_map:

Use this command to enable or disable the Network Map feature between copper trunk RI ports on token-ring modules.

- **show:**

  Is basically just a *read-only* command which enables the user to view the configuration parameters associated with the hub, such as individual modules, ports or trunks. Additionally you can view network, module, port, statistics counters and the error log information.

  Finally, you can also view usage information about the network paths and display a list of all the Ethernet source addresses for each frame received on a per port basis.

- **?:**

  The *?* lists available command and parameter options. For example, `save ?` lists the valid completions for the save command.

Only a subset of these commands can be executed from a terminal which has logged in as a *user*. The following is the list of these commands:

- Clear
- Logout
- Monitor
- Ping
- Remote_login
- Show

14.1.3 Ethernet Bridge Module - In-Band Management

From the Hub Display window, (refer Figure 151 on page 304), we can click anywhere on slot 6 to display a menu of the *in-band* management options for the Ethernet bridge module.

Note that clicking on the RS-232 for this module does not invoke a special form for terminal management as is the case for the Ethernet management module and the token-ring management module. A close inspection of Figure 151 on page 304 will show that the RS-232 port for the Ethernet bridge module is not highlighted in the same manner as that of the Ethernet management module or the token-ring management module.

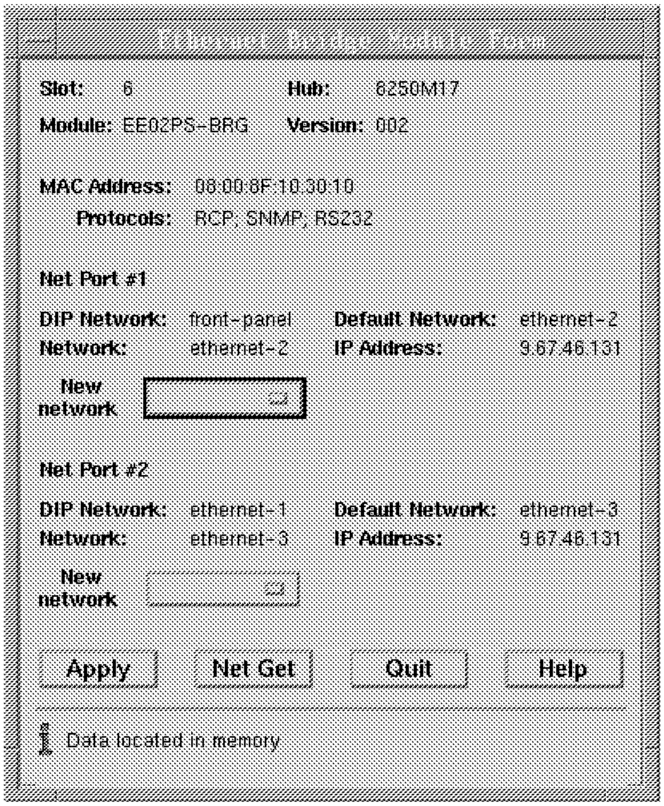
The implication of this, is that the Ethernet bridge module terminal can only be configured using *out-of-band* management. That is, the Ethernet bridge module terminal port can only be configured from either a direct attached terminal or from a remote-login session initiated from an Ethernet management module.

The Ethernet bridge **Management Module Menu** has the following options:

- Configuration
- Information
- Echo
- Ping
- Login
- Reset Module
- Help

14.1.3.1 Configuration

Selecting the *Configuration* option displays the **Ethernet Bridge Module Form**. See Figure 157 on page 325. This form allows you to configure the network to which each port of the bridge is connected.



Slot: 6 **Hub:** 6250M17
Module: EE02PS-BRG **Version:** 002

MAC Address: 08:00:8F:10:30:10
Protocols: RCP; SNMP; RS232

Net Port #1

DIP Network: front-panel **Default Network:** ethernet-2
Network: ethernet-2 **IP Address:** 9.67.46.131
New network

Net Port #2

DIP Network: ethernet-1 **Default Network:** ethernet-3
Network: ethernet-3 **IP Address:** 9.67.46.131
New network

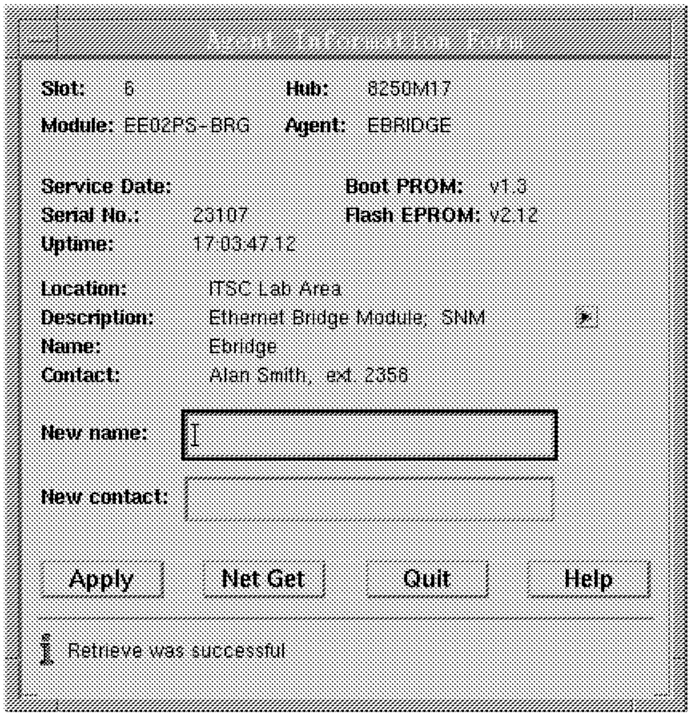
Data located in memory

Figure 157. The Ethernet Bridge Module Form. This is the main configuration form for the Ethernet bridge module.

Note that you can configure different IP addresses on each of the bridge ports should each port of the bridge module attach to a different IP network.

14.1.3.2 Information

Additional information about the Ethernet bridge module can be displayed by clicking the left mouse button on the *Information* option. See Figure 158 on page 326.



Slot: 6 Hub: 8250M17

Module: EE02PS-BRG Agent: EBRIDGE

Service Date: Boot PROM: v1.3

Serial No.: 23107 Flash EPROM: v2.12

Uptime: 17:03:47.12

Location: ITSC Lab Area

Description: Ethernet Bridge Module; SNM

Name: Ebridge

Contact: Alan Smith, ext. 2358

New name:

New contact:

Retrieve was successful

Figure 158. The Ethernet Bridge Agent Information Form

This form allows the administrator to set or modify the MIB-II variables **sysName** and **sysContact** by simply entering the desired information in the input fields corresponding to **Name** and **Contact**.

As for the Ethernet management module, the information in both the Configuration form and the Information form can be viewed using the AIX NetView/6000 *Browser* tool.

14.1.3.3 Echo

Clicking on the **Echo** option displays the **Echo Information Form** shown in Figure 155 on page 310.

This form enables the network administrator to send ICMP echo requests from the Ethernet bridge module agent to other IP addresses on the network. An ICMP echo request is more commonly referred to as the *ping* command.

The Echo Information Form also allows the administrator to set some of the parameters associated with the ICMP echo command.

The bit pattern sent in the ICMP packet can be specified by setting the **Pattern** parameter. Possible combinations are all zeros, all ones or mixed. Setting this pattern may be useful if you are using the IBM Trace program (or equivalent) to analyze the data flowing in your network.

You can also set the **Packet Size** parameter. The packet size must be between 64 and 1500 bytes in length.

Unlike the AIX HMP/6000 ping form, the echo form allows you to set the number of ICMP packets to be transmitted during the test.

14.1.3.4 Ping

Clicking on this option tests IP connectivity between the management station running AIX HMP/6000 and the selected Ethernet bridge module.

This test, however, is somewhat limited as only one ICMP packet is sent. If this packet is lost then the test fails. For a marginally better test you may consider pinging the Ethernet bridge module from either AIX NetView/6000 or the AIX command line as this will attempt to send ICMP packets in succession until explicitly stopped, thus providing a more accurate result.

14.1.3.5 Login

At the time of writing, the AIX HMP/6000 *Login* feature for the Ethernet bridge module was not available. This is because the Ethernet modules implement the remote login feature via a protocol called RCP (Remote Character Protocol) which uses the IEEE 802.2 link control layer. This protocol is not implemented by the AIX operating system.

The Ethernet remote login feature is somewhat limited because the RCP protocol is implemented only at the link layer which means it is not routable. This means that remote login sessions with Ethernet modules cannot be supported across IP routers.

The RCP protocol defines a master/slave relationship between the device initiating the login session and the device supporting the session respectively. Terminal characters are sent separately between the master and the slave. On completion of the command, the slave sends the output of the executed command.

RCP also monitors the session to determine if the session is still active. Basically the master pings the slave once every 60 seconds and should the slave fail to respond within the timeout period, the session is aborted.

The Ethernet bridge module does not support either Relnet or rlogin.

Do not confuse the *remote_login* command with the UNIX *rlogin* command; they are different.

Remote login is supported by the Ethernet management module and the Ethernet bridge module only.

14.1.3.6 Reset Module

Clicking on this option is equivalent to executing the command:

```
reset module 6
```

As described in the commands reference supplied with the Ethernet bridge module this command is normally only invoked when the module is not functioning as expected.

14.1.3.7 Help

Clicking on this option invokes the AIX HMP/6000 context sensitive help facility for the Ethernet bridge module.

14.1.4 Ethernet Bridge Module - Out-of-Band Management

Below is a list of those out-of-band commands that are executable by the administrator. Note, as many of the commands are similar to their Ethernet management module namesakes, only the variations will be defined below.

For complete command reference information refer to the documentation supplied with your 8250 bridge module.

14.1.4.1 Bridge Module Commands List

- **clear:**

  Used to delete an entry from the *community* table and to reset the *statistical counters* as well as clear the following configuration variables:

  filter:

  Used to erase an entry from the protocol ID table or the static address table. You must issue the `save filter` and `reset device` commands after modifying the tables for the changes to take effect.

  last_error:

  Used to clear the file that contains information on the last fatal error that occurred at the Ethernet bridge module.

- **help:**

  Use this command to get information about other commands.

- **maintain:**

  Used to enter maintenance mode for the out-of-band download.

  Note that there is no in-band download option for the Ethernet bridge module and hence the out-of-band download command has been implemented directly as a parameter of the maintain command.

- **monitor:**

  Used to view (monitor) ongoing performance statistics based on a selectable polling period.

  Note that the Ethernet bridge module monitors different statistics than the Ethernet management module.

- **remote_login:**

  Allows you to log in to another Ethernet bridge module, or an Ethernet management module This will provide you with an out-of-band management session on the remote device.

  You can only remotely log in one level down. That is, if you remotely log in to a device and you wish to remotely log in to another, you must log out of the first device before attempting to log in to the second.

- **set:**

  In addition to setting alert types and community names, the Ethernet bridge module supports the following parameters for the set command:

  bridge:

  Allows you to configure the following bridge specific parameters:

  ageing_time:

Sets the rate at which addresses are *aged* out of the dynamic filtering table.

This command does not affect the static address filter table.

channel:

Use this command to select the two Ethernet networks that you wish to bridge.

dip_configuration:

Determines whether the networks to which the Ethernet bridge module is configured, after the bridge module is reset or rebooted, are read from the hardware dip switch settings or from the settings specified by the management module.

side_switch_mode:

Enables or disables the bridge′s ability to detect when an Ethernet address in the address table has switched from one port to another.

device:

In addition to setting a device location, contact, name and password, and enabling device diagnostics, this command allows you to set the following parameters:

default_gateway_port1:

Specifies the IP address of the gateway that should be used when port 1 on the Ethernet bridge module tries to send IP packets to a receiver which is not on the same network as port 1.

default_gateway_port2:

Specifies the IP address of the gateway that should be used when port 2 on the Ethernet bridge module tries to send IP packets to a receiver which is not on the same network as port 1.

ip_address_port1:

Specifies the IP address for port 1 on the Ethernet bridge module.

ip_address_port2:

Specifies the IP address for port 2 on the Ethernet bridge module.

sqe_mode:

Enables the SQE errors to be displayed in the output of the `monitor` and `show` commands.

subnet_mask_port1:

Sets the subnet mask to be used with the network attached to port 1.

subnet_mask_port2:

Sets the subnet mask to be used with the network attached to port 2.

filter:

Allows the following parameters to be set:

mode protocol_id_table:

Sets the filtering mode that will be applied to protocol ID table.

protocol_id_table:

Allows you to add entries to the the protocol ID table.

static_address_table:

Allows you to add MAC addresses to the static address table and to set the forwarding rule to be applied to each entry.

spantree:

Allows you to change the spanning tree configuration parameters of the Ethernet bridge module:

bridge_priority:

This parameter is used in conjunction with the bridge MAC address to determine which bridge becomes the root bridge in the network.

forward_delay_time:

Sets the amount of time the bridge waits in each of the states when moving from listening to forwarding mode.

hello_address:

Modifies the address the bridge uses for the destination address of the hello BPDU.

Note that X′800143000000′ is the address defined by IEEE to be used for the hello BPDU. However, there are some older bridges in the market, which, although they supported spanning tree, used a different address. The bridge module allows you to change its hello address so that it can interoperate with these older bridges.

hello_time:

The frequency with which the bridge will send *hello* packets when it becomes the root bridge.

listen_time:

Specifies how long the bridge will wait for the root bridge to send a hello packet, before assuming that the root bridge has failed.

mode:

Enables or disables the bridge to take part in the spanning tree protocol.

path_cost_port1:

Sets the path cost of port 1 on the Ethernet bridge module.

path_cost_port2:

Sets the path cost of port 2 on the Ethernet bridge module.

Note that the Ethernet bridge module supports an out-of-band **help** command. This *help* command does not currently exist for either the Ethernet management module or the token-ring management module.

The subset of commands that are made available to the non-administrative user of the bridge module is as follows:

- Clear
- Logout
- Monitor

- Ping
- Remote_login
- Show

14.1.5 Ethernet Terminal Server Module - In-Band Management

From the Hub Display window, see Figure 151 on page 304, click the mouse anywhere on the Ethernet terminal server module in slot 14 to display a menu of management options for this module.

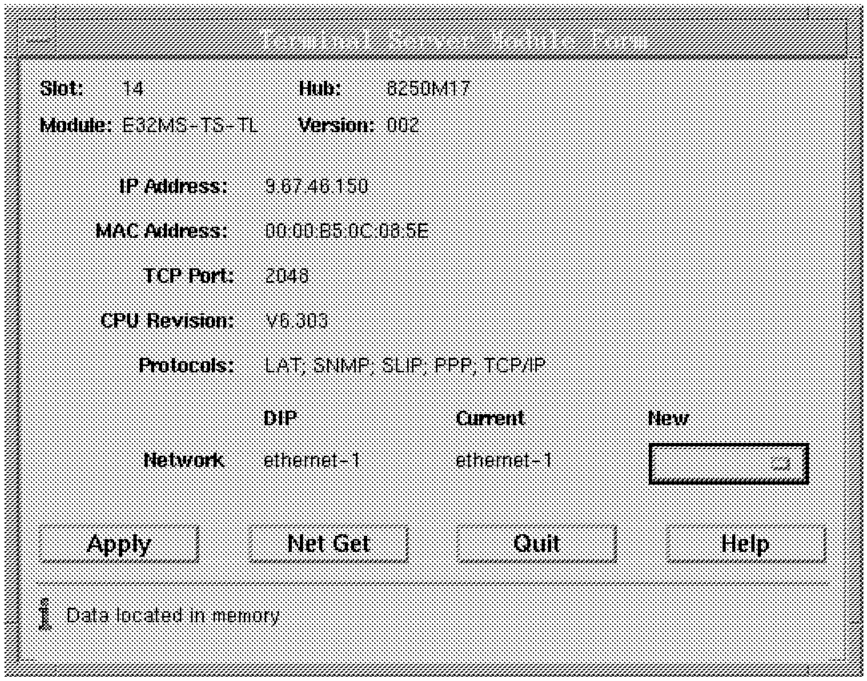
The Terminal Server **Management Module Menu** has the following options:

- Configuration
- Ports
- Ping
- Login
- Reset Module
- Help

Each of these is described in more detail below.

14.1.5.1 Configuration

Currently, in-band management of the Ethernet terminal server module is limited. As can be seen from Figure 159, the network to which the Ethernet terminal server module can be attached is the only configurable option. The form also provides a good deal of useful read-only information.



Terminal Server Module Form

Slot: 14 Hub: 8250M17
Module: E32MS-TS-TL Version: 002

IP Address: 9.67.46.150
MAC Address: 00:00:B5:0C:08:5E
TCP Port: 2048
CPU Revision: V6.303
Protocols: LAT; SNMP; SLIP; PPP; TCP/IP

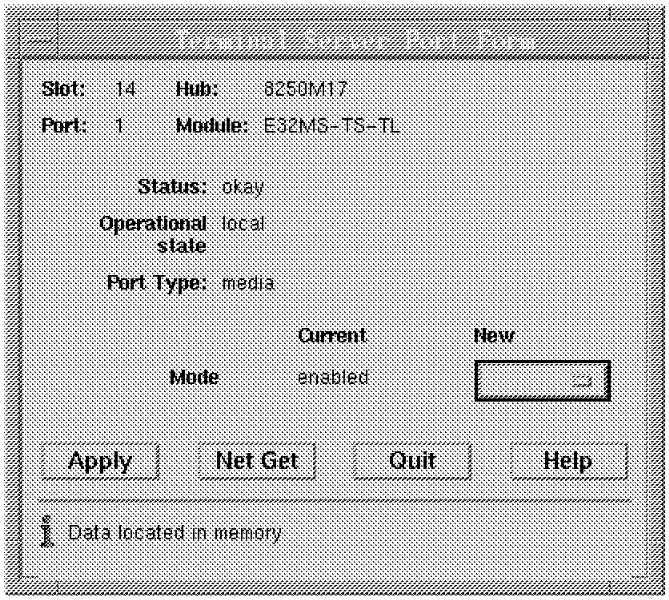
	DIP	Current	New
Network	ethernet-1	ethernet-1	

Data located in memory

Figure 159. The Ethernet Terminal Server Configuration Form. This is the main configuration form for the Ethernet terminal server module.

14.1.5.2 Ports

Selecting the *Port* option from the Terminal Server Management Menu will display a form similar to the one shown in Figure 160. This form is used to manage both physical and virtual ports.



Slot: 14 **Hub:** 8250M17

Port: 1 **Module:** E32MS-TS-TL

Status: okay

Operational state local

Port Type: media

	Current	New
Mode	enabled	

Data located in memory

Figure 160. The Ethernet Terminal Server Port Form. This is the configuration form for ports on the Ethernet bridge module.

The **Status** field indicates if there are signal problems with the port.

The **Operational state** may display any of the following values:

- **Idle:**

  Indicates that the port is not being accessed.

- **Local:**

  Indicates that the port is logged into the server and is able to access local services.

- **Connected:**

  Indicates that the port is accessing network services or is being accessed by the network.

The **Port type** field indicates whether the port is a **virtual** port or a **media** (physical) port.

The **Mode** field allows the port′s mode of operation to be configured. Valid modes are:

- **enabled:**

  Enables the port for both local and remote operations.

- **disabled:**

  The port is inoperative.

- **local:**

  Enables the port for operation with a local device only.

- **remote:**

  Enables the port for operation with a remote device only.

14.1.5.3 Ping

Clicking on this option tests IP connectivity between the management station running AIX HMP/6000 and the selected Ethernet terminal server module.

This test, however, is somewhat limited as only one ICMP packet is sent. If this packet is lost then the test fails. For a marginally better test you may like to consider pinging the Ethernet management module from either AIX NetView/6000 or the AIX command line as this will attempt to send ICMP packets in succession until explicitly stopped, thus providing a more accurate result.

14.1.5.4 Login

The login function for the Ethernet terminal server module is implemented using the **Telnet** virtual terminal protocol. Invoking this option opens a new AIXWindow running a terminal emulation of the Ethernet terminal server module console.

Note that the Ethernet terminal server module supports the Telnet protocol not the RCP (remote_login) which is used by the other Ethernet SNMP agent modules (Ethernet management module and Ethernet bridge module).

14.1.5.5 Reset Module

This option is normally only used when the module is not functioning correctly. It will perform a hardware reboot of the Ethernet terminal server module.

14.1.5.6 Help

Selecting this option invokes the AIX HMP/6000 context sensitive help facility for the Ethernet terminal server module.

14.1.6 Ethernet Terminal Server Module - Out-of-Band Management

Refer to Chapter 8, “Ethernet Terminal Server Module” on page 189.

14.2 Non-SNMP Agent Module Management

Provided you have a least one SNMP-enabled management module, all the non-SNMP agent Ethernet modules can be managed from AIX HMP/6000.

For information on the out-of-band management commands for these modules refer to the module documentation supplied with your 8250.

Issuing the equivalent in-band management commands from AIX HMP/6000 is relatively straight-forward. The forms corresponding to the module or port specific commands are invoked from the AIX HMP/6000 Hub Display window by clicking on the relevant module or port.

Below are some examples of these forms. We have not provided a complete list of possible forms as many of the differences are trivial.

14.2.1.1 An Example - The Transceiver Module

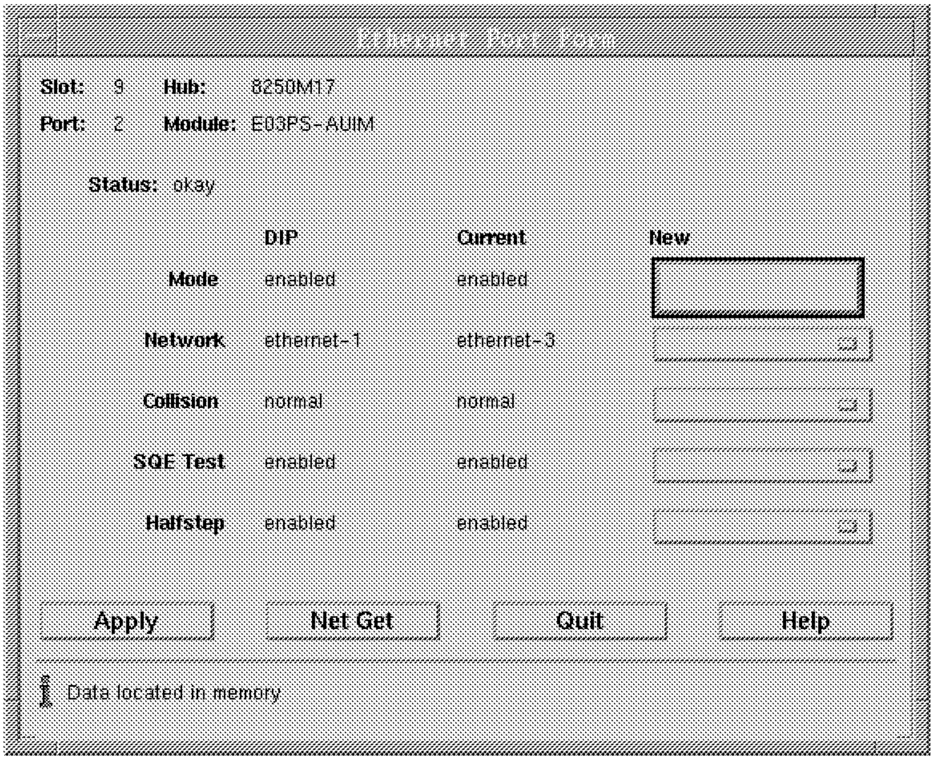
The AUI transceiver module is shown in slot 9 in Figure 151 on page 304. If you click anywhere on this module, other than on one of the three highlighted AUI ports, a simple menu will be displayed with the options:

- Reset Module
- Help

The *Reset Module* command simply executes a hardware reset of the module and is normally only invoked when the module is not functioning as expected.

There is no module configuration or information form for this module because the configuration is port specific.

However, if you click on one of the AUI ports, the Ethernet port form shown in Figure 161 is displayed.



Ethernet Port Form

Slot: 9 **Hub:** 8250M17

Port: 2 **Module:** E03PS-AUIM

Status: okay

	DIP	Current	New
Mode	enabled	enabled	
Network	ethernet-1	ethernet-3	
Collision	normal	normal	
SQE Test	enabled	enabled	
Halfstep	enabled	enabled	

Data located in memory

Figure 161. The Transceiver Module Ethernet Port Form

By selecting the appropriate *New* button you can enable or disable the port, configure the network to which it is attached and configure the following Ethernet specific parameters:

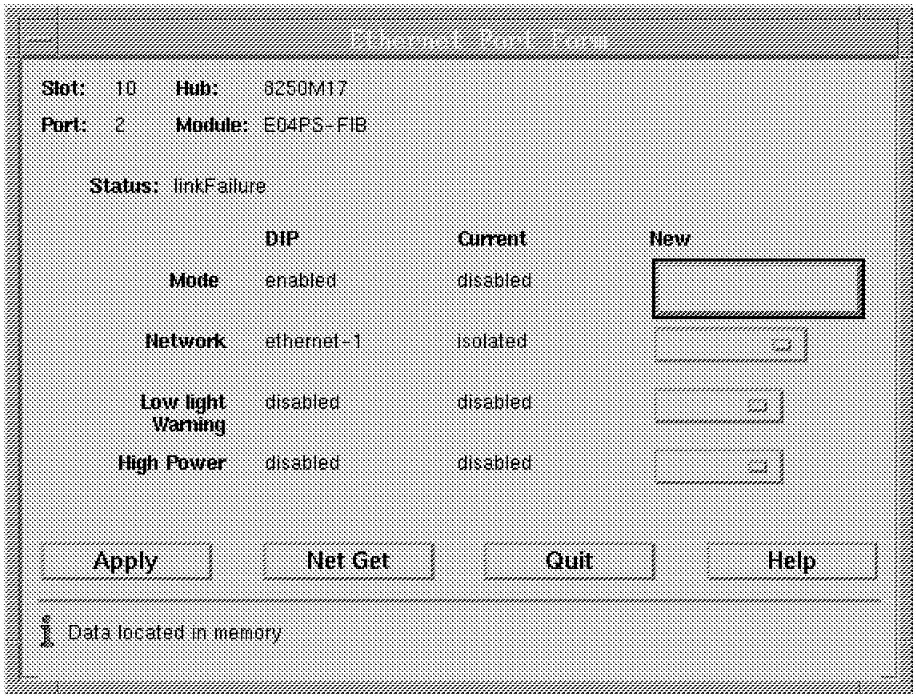
- The *collision* state
- Enable/disable SQE mode
- Enable/disable half-step signalling

For information about the transceiver module and the meaning of the above parameters, refer to 7.7, “Ethernet Transceiver Module” on page 158.

14.2.1.2 Another Example - The Ethernet Fiber Module

As for the transceiver module, configuration of the Ethernet fiber module is port specific; hence, clicking anywhere on this module invokes the simple menu with **Reset Module** and **Help** options only.

However, clicking on one of the fiber ports displays a different Ethernet port form; see Figure 162.



Ethernet Port Form

Slot: 10 Hub: 8250M17

Port: 2 Module: E04PS-FIB

Status: linkFailure

	DIP	Current	New
Mode	enabled	disabled	
Network	ethernet-1	isolated	
Low light Warning	disabled	disabled	
High Power	disabled	disabled	

Data located in memory

Figure 162. The Ethernet Fiber Module Port Form

Again, each port can be enabled or disabled and can be configured to a particular network. Additionally, the port can be configured to set off a warning, if a weak incoming light transmission is detected, and to enable high power transmissions if required.

For more information about configuring Ethernet fiber modules, refer to 7.2, “Ethernet Fiber Module” on page 130.

14.3 Statistics Gathering

The statistics gathering function of AIX HMP/6000 is invoked from the *Tools* menu of the Hub Display window. This section defines the statistical information that can be gathered for Ethernet networks and Ethernet module ports.

There are 8 counters used in gathering Ethernet statistics. They are outlined in Table 57 on page 336.

Table 57. Ethernet Traffic Statistics

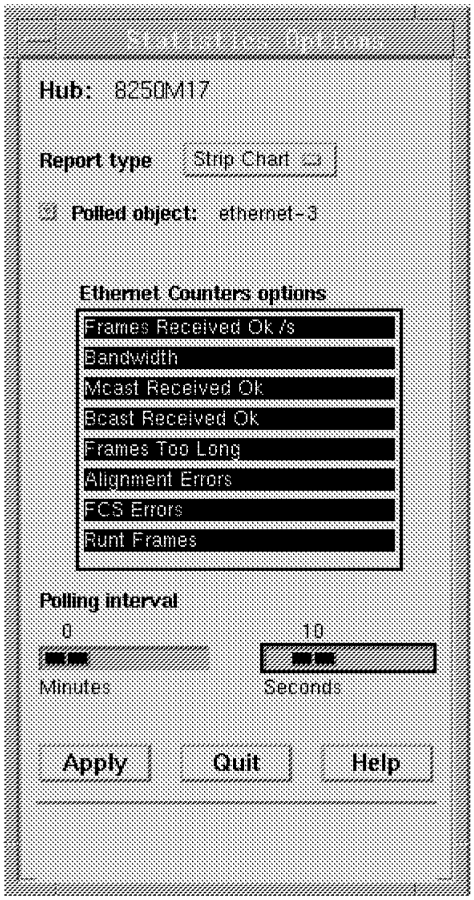
Counter Option	Description
FramesReceivedOk/Sec	Throughput rate shown as the number of good frames received per second.
Bandwidth	Number of good bits received per second divided by 10 million (theoretical maximum bandwidth).
McastReceivedOk	Number of good Multicast-Address packets received.
BcastReceivedOk	Number of good Broadcast-Address packets received.
FramesTooLong	Number of packets received greater than 1518 bytes.
AlignmentErrors	Number of frames that did not pass the Field Check Sequence checksum and are not an integral number of octets. This counter does not include FCS errors.
FCSErrors	Number of frames that did not pass the Field Check Sequence checksum and are an integral number of octets.
RuntFrames	Number of frames less than 512 bits long recorded over the remote network.

The first two counter options, *FramesReceivedOk/Sec* and *Bandwidth* in Table 57 are normalized with the length of the polling period. That is, they have the same units regardless of the polling period and as such can be compared for different polling period test sets. This is not the case for the remaining six counters.

The bandwidth counter is not particularly useful as it provides a fractional measurement of usage against a theoretical maximum. In reality, many Ethernet networks do not provide a real bandwidth anywhere near 10 Mbps hence this indicator may be quite erroneous.

14.3.1 An Example

From the **Tools** menu on the Hub Display window select **Statistics** to display the **Statistics Options** panel as shown in Figure 163 on page 337.



Statistics Options

Hub: 8250M17

Report type Strip Chart

Polled object: ethernet-3

Ethernet Counters options

- Frames Received Ok /s
- Bandwidth
- Mcast Received Ok
- Bcast Received Ok
- Frames Too Long
- Alignment Errors
- FCS Errors
- Runt Frames

Polling interval

Minutes: 0

Seconds: 10

Figure 163. The Statistics Options Form

This form allows you to set the type of output report, the network object to be analyzed, the parameters of that object to be gathered and the polling period which will be used to gather that information.

Using the **Report type** button we have selected a *Strip Chart* report. For this example we have selected all eight Ethernet statistics counters. These can be selected or de-selected simply by clicking on the corresponding counter option.

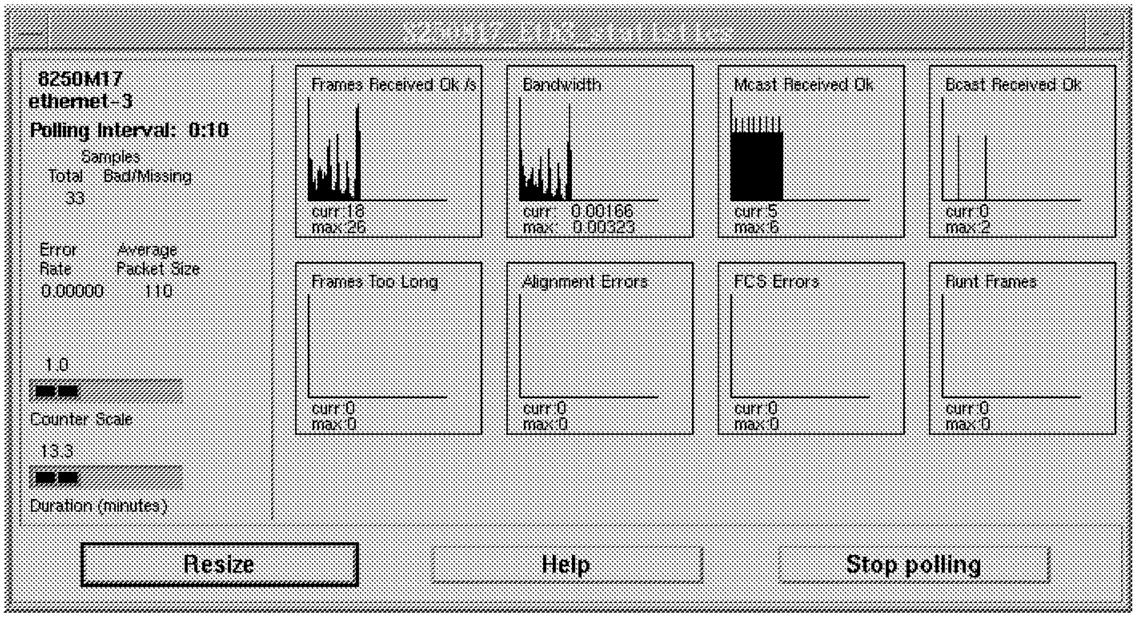
The **Polled object** button enables us to select a network or a specific port to be monitored. In this example we chose to monitor the *Ethernet_3* network.

The **Polling interval** slide bars allow you to select the frequency of the test samples. There is a bar for both minutes and seconds. Five seconds is the smallest allowable test interval.

The **Statistical Option** form showing our selections is shown in Figure 163.

Note that if you select a large number of objects to be polled, AIX HMP/6000 may limit the display to prevent excessive system load.

Now simply click on the **Apply** button to initiate the polling.



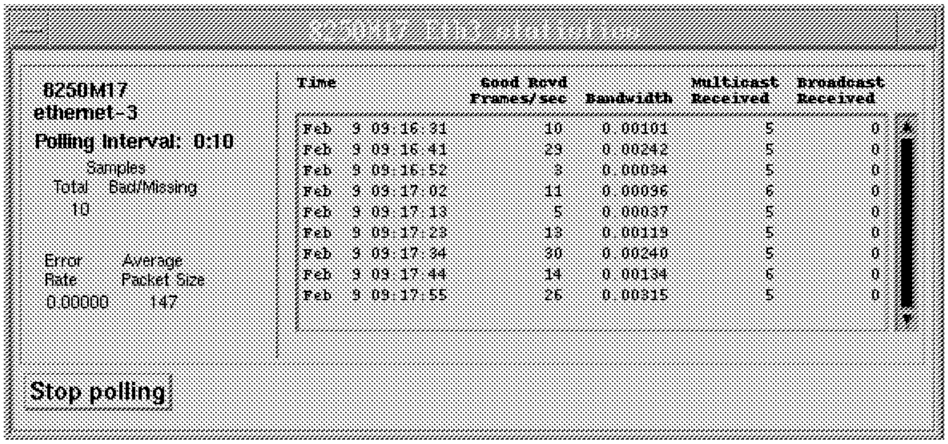
```
 8250M17
ethernet-3
Polling Interval:  0:10
        Samples
  Total   Bad/Missing
    33

 Error      Average
 Rate       Packet Size
 0.00000      110

  1.0
Counter Scale
  13.3
Duration (minutes)
```

Figure 164. An Ethernet Statistics Strip Chart Report

As a comparison we have shown the equivalent log report for the same test case in Figure 165 below. To get this output simply change the *Report type* parameter on the Statistics Options form to *Log report*.



```
 8250M17
ethernet-3
Polling Interval:  0:10
        Samples
  Total   Bad/Missing
    10

 Error      Average
 Rate       Packet Size
 0.00000      147
```

```
Time                   Good Rcvd              Multicast  Broadcast
                       Frames/sec  Bandwidth  Received   Received
Feb  9 09:16:31               10    0.00101          5          0
Feb  9 09:16:41               29    0.00242          5          0
Feb  9 09:16:52                3    0.00034          5          0
Feb  9 09:17:02               11    0.00096          6          0
Feb  9 09:17:13                5    0.00037          5          0
Feb  9 09:17:23               13    0.00119          5          0
Feb  9 09:17:34               30    0.00240          5          0
Feb  9 09:17:44               14    0.00134          6          0
Feb  9 09:17:55               26    0.00315          5          0
```

Figure 165. An Ethernet Statistics Log Report

For both report types the output samples commence at the end of the first polling interval.

In addition to the options you select from the Statistics Options form, the following information is also displayed:

- **Bad/Missing:**

  A counter of the number of invalid or missing samples.

- **Average Packet Size:**

An indicator of the average packet size in bytes per packet.

Also recorded, specific to each counter option, are the following:

- **Curr:**

  The number of frames in the current sample set.

- **Max:**

  The maximum number of frames received during the displayed sample period.

14.4 Access and Security

There are two areas aspects of network security for the 8250 Ethernet environment:

- Password security
- Address-to-port security

14.4.1 Password Security

There are two levels of password security that may be set for the Ethernet management module and the Ethernet bridge module:

Administrator Password: The administrator password provides both read and write access to all the commands. Use the following command to set the administrator password:

```
set device password administrator
```

User Password: The user password provides access to read-only commands. Use the following command to set the user password:

```
set device password user
```

For obvious security reasons the actual password is not echoed to the console when entered.

All passwords may contain up to 15 alphanumeric characters and are effective immediately though you must also issue the `save device` command for the new password to be permanently saved.

The password must be entered at the *Password:* prompt within 10 seconds or the terminal will timeout. If this happens, pressing the *Enter* key will re-display the prompt.

To discourage password guessing, after three invalid attempts, the console *sleeps* for thirty seconds before allowing another attempt.

14.4.2 Address-to-Port Security

Address-to-port security is only available from an advanced Ethernet management module.

The address-to-port security feature enables the Ethernet management module to assign known MAC address(s) to a specific port and to detect when an unauthorized MAC address attempts to connect to the network via that port.

If a MAC address other than the authorized addresses are detected on a secure port, the Ethernet management module will send an alarm to the Ethernet management module console and disable the port.

To set port security, you must first define the address to port mapping for each Ethernet port you wish to secure. For example:

```
set security port 12.4 mac_address 08-24-0F-00-2C-24
```

Having done this you then must enable the port security feature for those ports. This may be done on an individual port basis or for an entire module. For example, to enable security for port 4 in slot 12:

```
set security port 12.4 mode enable
```

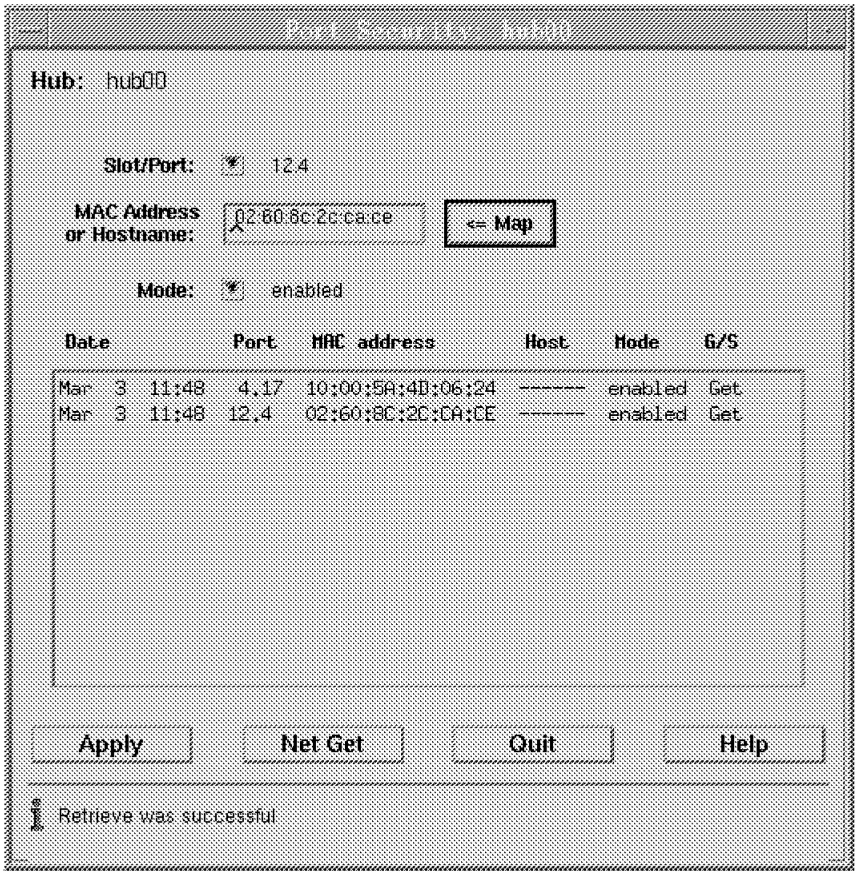
The same command can be used to disable port security.

More than one address can be assigned per port. In fact, a total of 1024 addresses per advanced Ethernet management module may be assigned to ports within a single 8250 hub.

An advanced Ethernet management module can be used to set port security for any Ethernet port within an 8250, even those on Ethernet networks to which the Ethernet management module is not connected. An Ethernet management module however cannot be used to set security for token-ring ports.

14.4.2.1 In-Band Port Security

Selecting the **Port Security** option from the *Tools* menu displays a form similar to the one shown in Figure 166 on page 341.



Port Security: hub00

Hub: hub00

Slot/Port: 12.4

MAC Address or Hostname: 02:60:8c:2c:ca:ce

Mode: enabled

```
Date            Port  MAC address        Host    Mode     G/S
Mar  3  11:48   4.17  10:00:5A:4D:06:24  ------  enabled  Get
Mar  3  11:48  12.4   02:60:8C:2C:CA:CE  ------  enabled  Get
```

Retrieve was successful

Figure 166. Port Security Form

This form allows you to use AIX HMP/6000 to view or update port security information for any port on a specific module.

The **Slot/Port** parameter allows you to select a specific port on a specific module. When selected, this parameter will only display module/port combinations which you can update.

The **Map** button retrieves the MAC address of the device attached to the port.

The **Mode** field allows you to **enable** or **disable** port security, **clear** a previously assigned address for this port or to perform **no change** when you only wish to view the results.

As can be seen from Figure 166, the port security form displays the following:

- **Date:**

  The date and time of the last operation on the port.

- **Port:**

  A fully qualified slot and port address.

- **MAC address:**

  The MAC address of the device assigned to the port.

- **Host:**

The name of the device attached to the port.

- **Mode:**

  The selected operation performed on the port.

- **G/S:**

  Specifies whether the activity was the result of an SNMP Get or Set operation.

Chapter 15. Token-Ring Management Functions

This chapter will look at token-ring management functions for the IBM 8250 Multiprotocol Intelligent Hub. The differences between *in-band* and *out-of-band* management of the token-ring management module will be highlighted.

While the examples in this chapter are documented in reasonable completeness, it assumed that the reader has a fundamental understanding of how to use both AIX HMP/6000 and the 8250 console terminal.

It is not the aim of this chapter to document every possible command for every token-ring module. Complete command reference material can be found in the documentation supplied with your modules.

This chapter will address the following sections:

- Configuration
- Non-SNMP Agent Module Management
- Statistics Gathering
- Access and Security

If you have not already done so, you may benefit from familiarizing yourself with the material covered in Chapter 12, " Hub Management - Before You Start" on page 275 before you progress any further.

15.1 Configuration

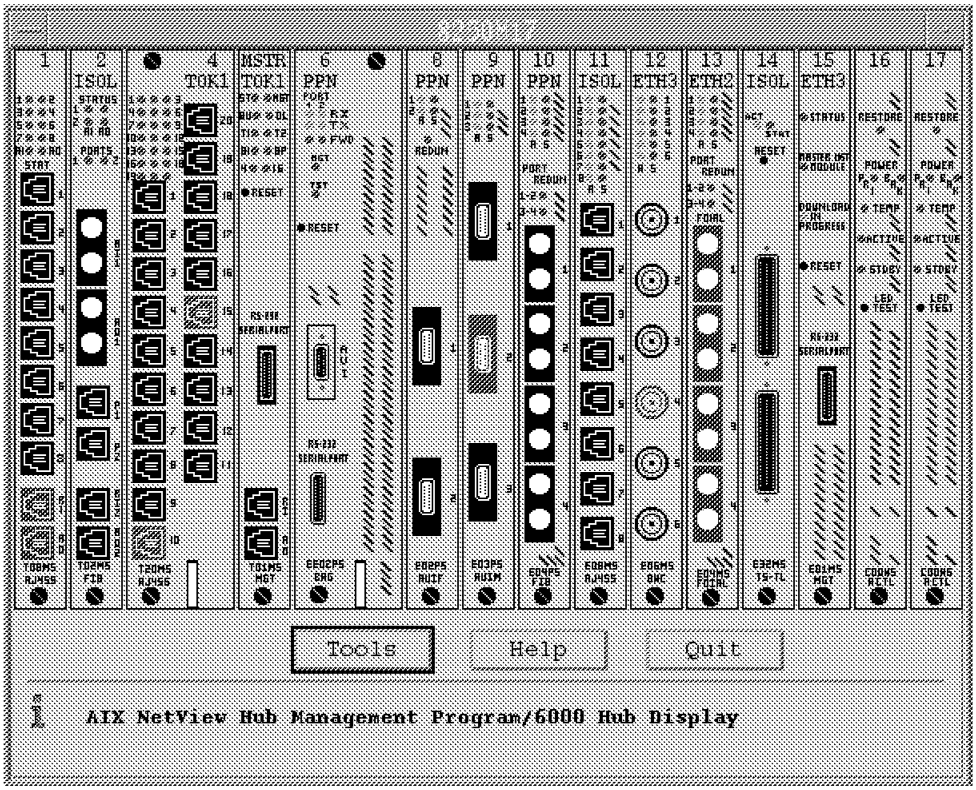
This section will look at the configuration management options for the 8250 token-ring modules. A table of the 8250 token-ring modules is shown in Table 58.

Table 58. 8250 Token-Ring Modules

Token-Ring Modules	**IBM Model Numbers**	**AIX HMP/6000 Identifiers**
Token-Ring Management	3823TM	T01MS-MGT
Token-Ring Twisted Pair MAU	3820T	T08MS-RJ45S
Token-Ring Twisted Pair Media	3821T	T20MS-RJ45S
Token-Ring Fiber Repeater	3822TR	T02MS-FIB

Remember that *in-band* management uses the SNMP and associated commands while *out-of-band* management includes only those commands entered from a direct RS-232 attached terminal console or pseudo-attached equivalent (a Telnet session for example).

For reference purposes we have reproduced the AIX Hub Display windows for each of the 8250s in our network; see Figure 167 on page 344 and Figure 168 on page 345.



AIX NetView Hub Management Program/6000 Hub Display

Figure 167. The AIX HMP/6000 Hub Display Window. The Hub Display window for the 8250 Model 17.

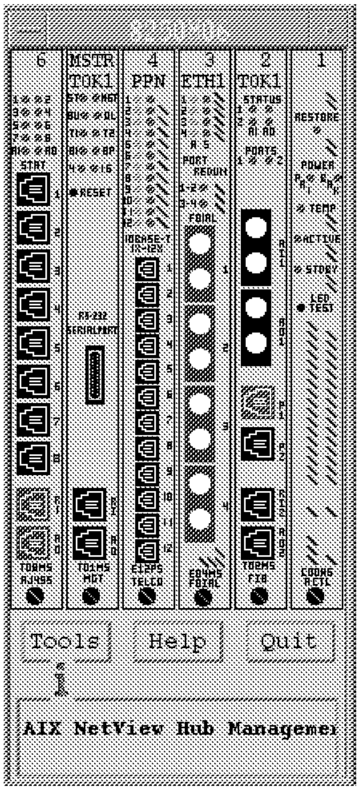


Figure 168. The AIX HMP/6000 Hub Display Window. The Hub Display window for the 8250 Model 6.

15.1.1 Token-Ring Management Module - In-Band Management

From the Hub Display window shown in Figure 167 on page 344, click the mouse anywhere on the token-ring management module in slot 5, except on the RS-232 port, to display the main menu of management options for this module.

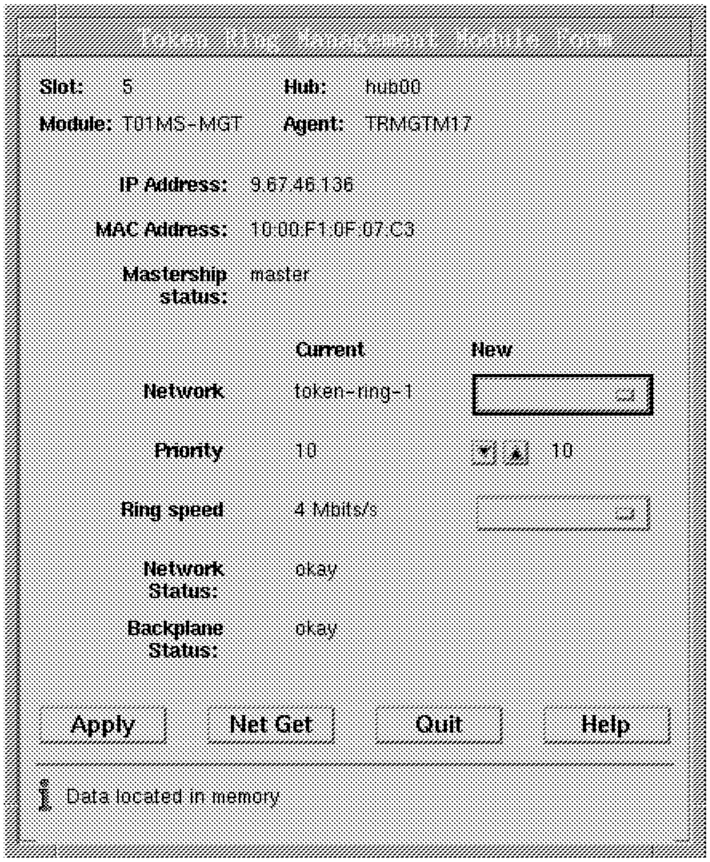
The token-ring **Management Module Menu** has the following options:

- Configuration
- Information
- Echo
- Ping
- Login
- Reset Module
- Download
- Help

Each of these is described in more detail below.

15.1.1.1 Configuration

Selecting the *Configuration* option displays the **Token-Ring Management Module Form**; see Figure 169. This form allows you to configure the network to which the module is connected, the mastership priority of the module and the ring speed setting.



Token-Ring Management Module Form

Slot:	5	Hub:	hub00
Module:	T01MS-MGT	Agent:	TRMGTM17

IP Address: 9.67.46.136

MAC Address: 10:00:F1:0F:07:C3

Mastership status: master

	Current	New
Network	token-ring-1	
Priority	10	10
Ring speed	4 Mbits/s	
Network Status:	okay	
Backplane Status:	okay	

Data located in memory

Figure 169. The Token-Ring Management Module Form. This is the main configuration form for the token-ring management module.

To configure the **network** to which the module is attached, click the mouse once on the *new* button in the form adjacent to the network parameter display. This will display a selection list of valid options from which you can choose.

The list of available network options is determined by the configuration of the remainder of the hub.

Refer to 6.2, “Advanced Backplane Architecture” on page 109 for a detailed explanation of the IBM 8250 Multiprotocol Intelligent Hub backplane architecture which dictates the allowable network mix on the hub.

The *up-arrow* and *down-arrow* buttons allow you to increase or decrease the **mastership priority** of the token-ring management module. This parameter is used by the mastership election process to determine which module becomes the hub master when there are multiple management modules (token-ring and/or Ethernet) in the same hub.

A mastership election may be invoked for a number of reasons, such as the execution of the reset mastership command, a power failure in the hub, execution of the reset concentrator command or failure of the current master.

The highest priority is 10 decreasing to the lowest, 1. The election process is most efficient if the intended master has a priority of 10 and all other management modules have a lower priority.

If more than one management module has the same priority, then the results of a mastership election are unpredictable. The first to complete initialization will become the master and the remaining management modules will be slaves.

In addition to the *warnings* highlighted below you should think carefully about the implications of your management module priority settings.

Consider the implications of a scenario where the intended slave management modules have a configuration different from the intended master module and the master fails.

For example, say we have two management modules each with different configuration parameter settings in their non-volatile memory from previous a *save* command. If you assign both the intended master and the intended slave the same priority, then after the power-on, the intended slave may become the master which will result in the 8250 being configured in a way other than was planned and expected.

This is only a single example of which there are many, so care must be exercised in assigning mastership priority to the management modules.

WARNING

At this level of microcode a mastership election will result in an Ethernet management module becoming the master ahead of a token-ring management module regardless of the mastership priorities set in each module, given the following conditions:

- The token-ring management module has *diagnostics enabled* **and**
- The mastership election was *not* invoked by the reset mastership command, **and**
- The token-ring management module is at microcode level 1.10 -B **and**
- The Ethernet management module is at microcode level 3.1 -A

The reason for this is the longer time the token-ring management module requires to run diagnostics during startup versus the initialization time of the Ethernet management module. That is, the Ethernet management module is wrongly allowed to assume mastership because the token-ring management module has not had sufficient time to establish itself as a mastership contender.

The reset mastership command does not cause the token-ring management module to reboot, (and hence run diagnostics), therefore, it does not cause this anomaly.

Note that the token-ring management module factory default enables diagnostics.

To fix this problem ensure that the token-ring management module has a higher priority than the Ethernet management module and execute the following commands from the token-ring management module console or pseudo-console equivalent:

```
set device diagnostics disable
```

```
reset mastership
```

Unfortunately, none of the AIX HMP/6000 token-ring forms display the current setting of the *diagnostics* parameter. To find out about the diagnostics setting for the token-ring, you will need to use the `show device` command from the token-ring management module console or pseudo-console equivalent (a Telnet session).

WARNING

At the following levels of microcode if the Ethernet management module is allowed to become the master, it will not be able to recognize token-ring management modules, thus rendering them useless.

- Token-ring management module at microcode level 1.10 -B
- Ethernet management module at microcode level 3.1 -A

Normally, where a token-ring management module and Ethernet management module are to coexist in the same 8250, it is recommended that the token-ring management module be configured as the master. This is to ensure that the full functionality of the token-ring management module is accessible, (such as beacon recovery for example).

If an Ethernet management module becomes the master when a token-ring management module is present, you can correct the situation by doing the following:

1. Ensure that the token-ring management module has a greater mastership priority than the Ethernet management module. To change the token-ring management module mastership parameter you must have a console attached directly to the token-ring management module as it is isolated and the Ethernet management module is unable to recognize the token-ring management module.
2. Issue the `reset mastership` command and allow the token-ring management module to become the master and the Ethernet management module the slave.

The other parameter you can configure from the *Token=Ring Management Module Form* is the **ring speed**. To configure the ring speed parameter, simply click on the button corresponding to this field in the form. Valid selections (4 Mbps or 16 Mbps) will be displayed.

All other parameters in the *Token-Ring Management Module Form* are read-only. You should especially note that you cannot change parameters such as the agent IP address for the token-ring management module via AIX HMP/6000.

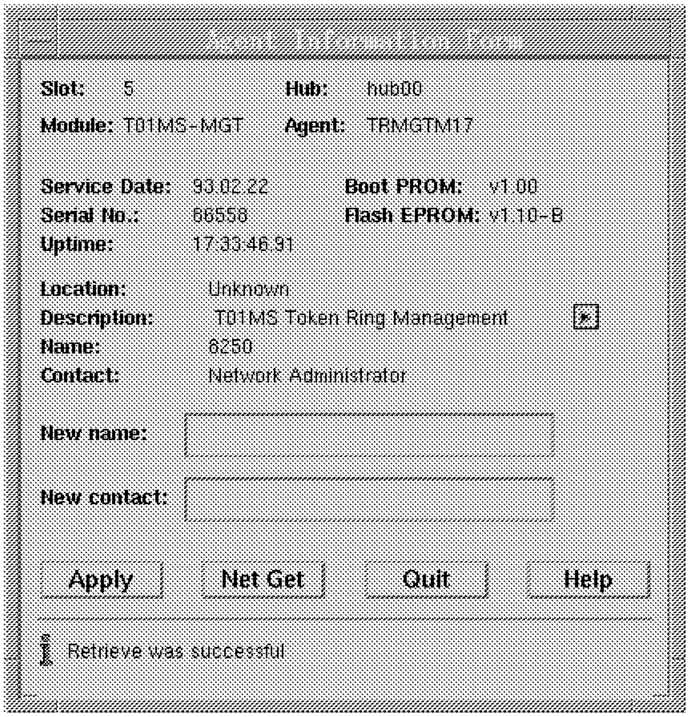
This means that the setup required for establishing IP connectivity between the SNMP network manager and the token-ring management module must be accomplished (at least in part) with a direct-attached asynchronous ASCII terminal.

See Chapter 12, “ Hub Management - Before You Start” on page 275 for more detail on initial setup requirements.

15.1.1.2 Information

Additional information about the the token-ring management module can be displayed by clicking the left mouse button on the *Information* option.

Again, this form, see Figure 170, provides mostly read-only information.



Agent Information Form

Slot:	5	**Hub:**	hub00
Module:	T01MS-MGT	**Agent:**	TRMGTM17
Service Date:	93.02.22	**Boot PROM:**	v1.00
Serial No.:	86558	**Flash EPROM:**	v1.10-B
Uptime:	17:33:46.91		

Location:	Unknown
Description:	T01MS Token Ring Management
Name:	8250
Contact:	Network Administrator
New name:	
New contact:	

Retrieve was successful

Figure 170. The Token-Ring Agent Information Form. This is primarily an information form for the token-ring management module.

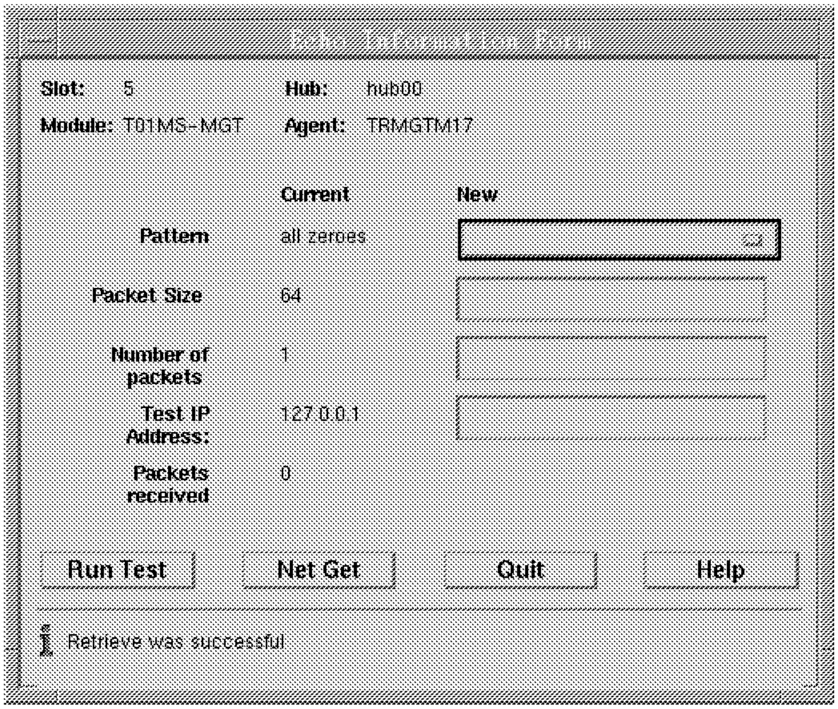
The agent *Name* and *Contact* information may be altered in this form by clicking the left mouse button in the corresponding input field for each parameter and entering the desired change.

These fields correspond to the standard MIB-II variables **sysName** and **sysContact**.

The information in both the Configuration form and the Information form can also be viewed via the *MIB Browser* under the *Tools* menu of *AIX NetView/6000*. In fact, this tool can be used to alter the *Location* field in the Information form as it corresponds to the *sysLocation* variable in the standard MIB-2 database and has write permission. All other fields however are read-only MIB variables.

15.1.1.3 Echo

Clicking on the **Echo** option displays the **Echo Information Form** shown in Figure 171.



Echo Information Form

Slot: 5 Hub: hub00

Module: T01MS-MGT Agent: TRMGTM17

	Current	New
Pattern	all zeroes	
Packet Size	64	
Number of packets	1	
Test IP Address:	127.0.0.1	
Packets received	0	

Retrieve was successful

Figure 171. The Echo Information Form

This form enables the network administrator to send ICMP echo requests from the token-ring management module agent to other IP addresses on the network. An ICMP echo request is more commonly referred to as the *ping* command.

The Echo Information Form also allows the administrator to set some of the parameters associated with the ICMP echo command.

The bit pattern sent in the ICMP packet can be specified by setting the **Pattern** parameter. Possible combinations are all zeros, all ones or mixed. Setting this pattern may be useful if you have an IBM Trace program (or equivalent) available to analyze your network traffic.

You can also set the **Packet Size** parameter. The packet size must be between 64 and 1500 bytes in length.

Unlike the AIX HMP/6000 ping form, the echo form allows you to set the number of ICMP packets to be transmitted during the test.

15.1.1.4 Ping

Clicking on this option tests IP connectivity between the management station running AIX HMP/6000 and the selected token-ring management module. An ICMP echo request is sent from the AIX HMP/6000 management station to the token-ring management module.

This test, however, is somewhat limited as only one ICMP packet is sent. If this packet is lost then the test fails. For a marginally better test you may consider pinging the token-ring management module from either AIX NetView/6000 or the AIX command line as this will attempt to send ICMP packets in succession until explicitly stopped, thus providing a more accurate result.

15.1.1.5 Login

The login function for the token-ring management module is implemented using the **Telnet** virtual terminal protocol. Invoking this option opens a new *AIXWindow* running a terminal emulation of the token-ring management module console.

This session will prompt you for a password to allow you to log on to the token-ring management module. A Telnet session will allow you to perform exactly the same commands as you would from a direct-attached terminal console; hence, even though the session was invoked from AIX HMP/6000 it is classified as out-of-band management because it is not using the SNMP.

A Telnet session could also be invoked from the AIX command line.

15.1.1.6 Reset Module

Clicking on this option is equivalent to executing the command:

```
reset module 5
```

As described in the commands reference supplied with the token-ring management module this command is normally only invoked when the module is not functioning as expected.

Prior to issuing the `reset module` command you should execute the `save all` command to ensure that current changes are not lost.

Be aware that invoking this command will generate approximately 24 error windows to AIX HMP/6000 instructing that hub rediscovery may be necessary.

15.1.1.7 Download

Display the **Download Form** by clicking on this option. This form allows you to set the parameters required to download new microcode to the token-ring management module. The new code may be a new version (*boot code*) or a release/modification update (*flash code*).

The documentation for the in-band download command supplied with the token-ring management module indicates that the TFTP (Trivial File Transfer Protocol) parameters must be explicitly set using the `set tftp` command before you can execute an in-band download.

This is not the case when an in-band download is initiated from AIX HMP/6000. The AIX HMP/6000 download form provides input fields for the TFTP parameters which renders this requirement superfluous.

The in-band download procedure that we used to update the flash code level of the token-ring management module in the 8250 Model 6 is detailed below:

1. Make an AIX directory to store the image to be downloaded. We created a directory called *download* under the */usr/etc/hmp* directory. This is arbitrary; you could use any directory you wish. To do this execute the following AIX commands:

```
cd /usr/etc/hmp
mkdir download
```

2. Copy the image file to be downloaded from the diskette to the /usr/etc/hmp/download directory that you created in step 1. Note that the diskette is formatted for DOS or OS/2 not AIX so you will need to use the AIX `dosread` command.

   The DOS filename in this example is *TRMM111.BIN*. If required, the DOS `dir` command can be used to read the contents of the diskette.

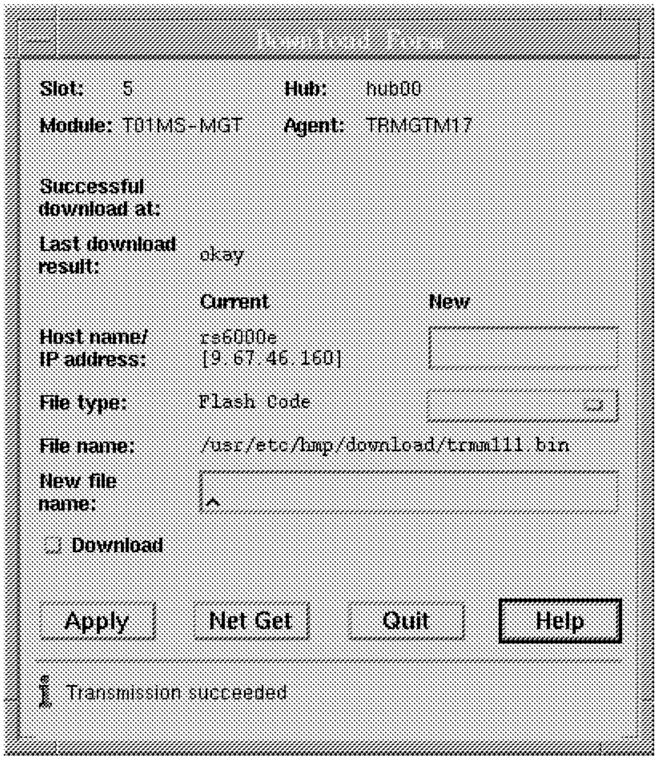
   To read the file into the AIX file system, change to the target directory and copy the file:

   ```
   cd /usr/etc/hmp/download
   dosread trmm111.bin trmm111.bin
   ```

   The dosread command parameter syntax is *source* then *destination* so the effect of this command will be to create a file image of the same name. This name is arbitrary if you wish to rename it.

3. If you have not already done so, invoke the *download* form from the token-ring management module menu.

   The download form will look similar to the one shown in Figure 172. This figure shows the parameter settings used in this example.



Download Form

Slot: 5 Hub: hub00

Module: T01MS-MGT Agent: TRMGTM17

Successful download at:

Last download result: okay

	Current	New
Host name/ IP address:	rs6000e [9.67.46.160]	
File type:	Flash Code	
File name:	/usr/etc/hmp/download/trmm111.bin	
New file name:		

□ Download

Transmission succeeded

Figure 172. The Download Form. The parameter settings displayed in this figure were used for this example.

4. Set the download form parameters.

Set the **Host name/IP address** parameter to the IP address of your RISC System/6000 which you wish to download from.

In this example the **File type** was flash code. The IBM documentation supplied with the software should indicate what type of update it is.

Note that the file type parameter is valid only for the token-ring management module. It is not an option for the Ethernet management module.

Set the **File name** of the AIX file which you wish to download. This should (obviously) be consistent with the file name you created in step 2.

5. Activate the Download button.

   The download button is merely a safety check that forces you to explicitly confirm that you wish to perform the download with the current parameter settings.

   Clicking on the download button will not initiate the download. The button will turn dark gray when active.

6. Initiate the download.

   To start the download process click on the *Apply* button.

   If you did not activate the Download button (see previous step) this will simply send an SNMP *set* command to the token-ring management module agent to change the current MIB values corresponding to the parameters in the form.

During the download, (which for this example only took about 2 minutes), you will lose connectivity with the agent. This is indicated by a message in the Hub Display window. When the download is complete a message indicating that connectivity has been re-established will also be displayed.

If you attempt to perform a *Net Get* from a form during the download you will also get an error message in the form indicating a timeout error. These errors are nothing to be concerned about.

15.1.1.8 A Caution

Although we did not experience the following problem with the in-band download procedure it has been experienced by others, so it is worthy of mention here.

There is a MIB variable called **tftpStart** which dictates whether or not, and in which direction, the TFTP file transfer will execute. This variable is of type **integer** and supports the following values:

- **tftpNoTransfer (1):**

  Do not perform a transfer.

- **tftpGet (2):**

  Transfer to the agent - download.

- **tftpPut (3):**

  Transfer to the server - upload.

To perform a download the tftpStart variable must be set (obviously) to 2.

Sometimes it is required that this variable be explicitly set before attempting the download. Unfortunately, at the time of writing, the cause of this anomaly was unknown.

There are two ways of setting this variable. It can be altered using the AIX NetView/6000 *Browser* tool or it can be set by issuing the following SNMP command:

```
snmpset node community .1.3.6.1.4.1.49.2.6.1.0 integer 2
```

The *node* parameter should be the name or IP address of your agent and the *community* parameter should be valid for that same agent. The dotted decimal parameter is the MIB identifier for the tftpStart variable.

15.1.1.9 Help

Selecting this option invokes the AIX HMP/6000 context sensitive help facility for the token-ring management module.

15.1.2 Token-Ring Management Module - Out-of-Band Management

Essentially there are two ways of performing out-of-band management with the token-ring management module:

- A terminal connected directly to the token-ring management module′s RS-232 port

  The terminal may be attached locally or remotely via modem. It could also be a PS/2 running suitable terminal emulation software such as IBM′s FTTERM (File Transfer and Terminal Emulation Program).

- A remote pseudo-terminal session via the Telnet virtual terminal protocol

Once connectivity has been established between the token-ring management module and the console you can log on either as an administrator or a user. Refer to 15.4, “Access and Security” on page 369 for more information on passwords and security.

The following out-of-band commands are executable by the administrator from the token-ring management module console:

15.1.2.1 Token-Ring Management Module Commands List

- **boot:**

  This command is used to return from maintenance mode and to boot the operational code in the flash EPROM. This command is only available from maintenance mode.

- **clear:**

  This command is used to reset or clear the following configuration variables:

  community:

  Deletes an entry in the community table.

  counter:

  Clears the statistical counters.

  error_log:

  Erases the error log.

  security port:

  Enables you to clear the port′s MAC address and disable security.

  tftp result:

Clears the TFTP result from the *show tftp* command display. This should be used before you begin an in-band download.

- **download:**

  Performs both *in-band* and *out-of-band* loading of new token-ring management module software.

  In-band download is available in both maintenance and normal mode.

  Out-of-band download is available *only* in maintenance mode.

- **logout:**

  Terminates the current session.

  If you are logged into a remote token-ring management module or another device, this command will terminate the connection to the remote device and will re-establish a connection with the local token-ring management module.

  If the connection is via a modem and the *hangup* parameter is *enabled* then the logout command also disconnects the modem.

- **maintain:**

  Enters maintenance mode.

- **monitor:**

  This command is used to view (monitor) ongoing performance statistics based on a selectable polling period.

- **ping:**

  This command is used to test connectivity between the token-ring management module and another IP addressable device on the network.

- **reset:**

  This command allows you to refresh or reassign the following:

  concentrator:

  Allows you to reboot both the hardware and the software (cold boot) of the 8250 hub.

  Diagnostics will be executed for those modules which have the *diagnostics* parameter enabled.

  Note that you must save or revert any unsaved changes before this command will execute.

  device:

  Resets the token-ring management module to which you are logged into.

  Note that you must save or revert any unsaved changes before this command will execute.

  mastership:

  Will force a mastership re-election in hub.

  module:

  Will perform a hardware reset of the module. This command should only be used if a module is not functioning correctly.

  You cannot reset the controller module using this command; you must use the *reset concentrator* to do this.

You cannot reset the token-ring management module to which you are logged on to; you must use the *reset device* to do this.

power_supply:

This command is used in a situation where the hub is working off the backup power supply. It will cause a switch from the backup power supply to the the primary power supply.

Note that you must save or revert any unsaved changes before this command will execute.

A power supply switch performs a warm boot which causes the hub and all the modules to reset.

- **revert:**

  Use this command to return the configuration to the settings that were in effect as of the last save. It is possible to revert selected parameters. However, *revert security* and *revert tftp* options are only available for the advanced Ethernet management module.

- **save:**

  Saves the current configuration values established by the *set* command. It is possible to save selected parameters.

  Note that only the *saved* values are effective upon a reset.

- **set:**

  Enables you to change configuration values. Following is a list of those parameters:

  alert:

  Allows you to enable or disable the notification of an alert (trap) type to an SNMP management station such as AIX NetView/6000.

  The following three alert types are valid:

  1. **authentication:**

     This trap is issued when an SNMP request is received from a network manager whose IP address or community name is not valid for the attempted operation.

  2. **change:**

     Issued when any configuration change is made to this hub.

  3. **hello:**

     When an existing token-ring management module is reset, this trap is sent once every minute until a valid SNMP PDU (Protocol Data Unit) is received or for up to 4 hours and 15 minutes, at which time the token-ring management module stops sending the trap.

  clock:

  Sets the real-time clock.

  community:

  Creates entries in the community table for network management stations that will issue SNMP requests or receive traps from this token-ring management module.

  concentrator platform:

Use this command to inform the token-ring management module of the hub platform in which it is installed.

The default setting is the 8250 Model 17. If you do not reset this parameter for the 8250 Model 6, AIX HMP/6000 will depict it as a Model 17.

device:

Allows you to configure the parameters listed below:

contact:

A textual string describing the person responsible for the module/hub.

default_gateway:

Used to set the IP address of the gateway that should be used when the token-ring management module does not recognize an address on the local network.

This parameter is useful when sending traps to a management station on a different network. It is possible to configure a separate gateway address each of the seven possible token-ring networks on the backplane.

diagnostics:

Enables or disables diagnostics during a boot of the token-ring management module.

dip_configuration:

Allows the module to boot according to either the settings of the hardware dip switches or the software settings.

ip_address:

Use this command to set the token-ring management module′s IP (Internet Protocol) address. A unique IP address can be configured for each token-ring on the backplane.

Note that for the IP address to take effect it is necessary to execute the following commands after changing the IP address:

```
save all
```

```
reset device
```

Location:

A textual string describing the location of the module/hub.

name:

A symbolic name that may be used instead of the IP address.

password:

Establishes a security password for an administrator and/or user.

subnet_mask:

Used to specify the subnetwork mask that is to be used for local subnetting. Refer to 4.2, "IP Addressing" on page 74 for an explanation of subnetting.

You can configure a unique subnet mask for each token-ring network on the backplane.

trap_receive:

Use this command to enable this token-ring management module as a trap receiver for other SNMP devices on the network.

module:

Enables you to configure the following module parameters:

cable impedance:

Use this command to set the cable impedance level for token-ring module lobe ports.

You should set the cable impedance for Unshielded Twisted Pair to 100 ohms and for Shielded Twisted Pair to 150 ohms.

crossover:

Enables/disables crossover mode for port 8 of the 10BASE-T module. Note that when connecting two 10BASE-T modules, one port must be crossed and the other uncrossed.

fifo_fill_level:

Controls the number of bits loaded into the internal FIFO buffer before the bits are unloaded.

This command is only applicable to certain older twisted pair products that have FIFO capability. This is not applicable to any of the modules marketed by IBM for the 8250.

low_light_warning:

When enabled, the low-light warning LED will indicate (6 blinks) that a weak light signal is being received from an Ethernet fiber module.

mastership priority:

Sets the priority level of the module in the event of a mastership election.

module_bypass:

Use this command to insert token-ring MAU modules into a ring to which the RI and RO cables of the MAU are connected. When set to *bypass*, ring traffic still passes through the MAU′s RI/RO ports but not the eight lobe ports. This is automatically set to bypass mode when the MAU is placed in a hub where there is an operational management module.

network:

Assigns the module to a particular network.

ring_speed:

Enables you to set the module to operate at a transmission rate of either 4 Mbps or 16 Mbps for token-ring networks.

port:

Allows you to configure the following port-specific parameters:

collision:

The collision mode may need to be set to *alternate* if used with non-IEEE 802.3 devices. *Normal* mode is used for IEEE 802.3 devices.

half_step:

Enables half-step signalling for ports on the transceiver module. Half-step enabled is the default setting and is used for IEEE 802.3 and Ethernet Version 2.0 devices. Early Ethernet and non-802.3 devices may require full-step signalling.

high_power:

Enables or disables the port from receiving or transmitting at high power. This command pertains to the Ethernet port switching fiber modules only.

link_integrity:

The 10BASE-T standard requires that link integrity be enabled. Some older non-10BASE-T equipment may require that you disable link integrity on the port.

This parameter must be set to the same value at both ends of the link.

low_light_warning:

When enabled the port will indicate the receipt of weak signals by blinking a certain number of times. For the number of blinks, refer to the appropriate module′s description in Chapter 7, "8250 Ethernet Modules and Accessories" on page 129.

This command pertains only to the Ethernet port switching fiber modules.

mode enable/disable:

Use this command to explicitly turn a port on or off.

mode local/remote:

This command allows you to configure the port access for the Ethernet terminal server module. Set this parameter to *remote* if the port will be accessed from a remote device via a modem for example. The default setting is *local*.

mode redundant/non_redundant:

Establishes redundancy between two ports. One port is established as the primary link and the second becomes a backup in the event of a failure on the first. Port redundancy can be set across modules as well.

mode remote_diagnostics/non_remote_diagnostics:

Use this command to establish a the Remote Diagnostics protocol on a pair of 10BASE-T ports. This protocol enables the module to work dynamically with an IBM fault-tolerant 10BASE-T transceiver to sense problems and switch automatically to a backup link.

Note that you must have link integrity enabled on the transceiver for this command to work correctly. Link integrity will automatically be enabled on the module when you enable remote diagnostics for that module.

This feature currently works on the Ethernet 50-pin module only.

mode remote_failure_signalling:

Establishes remote failure signalling on redundant FOIRL links.

network:

Assigns the port to a specific network.

receive_jabber:

Can be enabled for the Ethernet 50-pin module. When enabled, if a jabber condition occurs and the transceiver or repeater device fails to halt it, the token-ring management module will protect the network by disconnecting the link after 10 msecs.

The default setting is disabled to conform with the 10BASE-T standard.

sqe_test:

Enables or disables the SQE test for ports on the Ethernet transceiver module. The SQE test normally needs to be disabled to allow this port to connect to either a baseband repeater or multiport transceiver.

squelch:

May be set to either *normal* or *low*. It is factory set to normal to comply with the 10BASE-T standard.

A low squelch level will allow the module to sense a weaker signal allowing a longer link distance between two modules; however, this increases the risk of losing packets due to impulse noise.

station_type:

Use this command to define the ports which have stations that assert a phantom presence but not a MAC presence. An example of such a station is the IBM Token-Ring Network 16/4 Trace and Performance adapter.

security:

Enables the configuration of the following security parameters:

port mac_address:

Used to define address-to-port security on individual ports. Once a MAC address is set for a specific port and the security is enabled (see *set security port mode* command), if the token-ring management module detects a change in a port′s source MAC address, it will send an alarm to the token-ring management module console or a trap to an SNMP network management station, and shut down the port. Multiple MAC addresses may be assigned to the same port.

port mode:

Enables security for a port which has been assigned a MAC address(es) using the *set security port mac_address* command.

terminal:

Enables the configuration of the following parameters for the terminal console RS-232 port:

baud:

Sets the transmission rate of the token-ring management module RS-232 port.

data_bits:

Sets the number of data bits used in the transmission.

hangup:

Used to automatically disconnect a modem attached to the RS-232 port when you log out.

parity:

Establishes the parity setting to use during transmission.

prompt:

Allows you to customize the prompt you receive at your token-ring management module console.

stop_bits:

Establishes the number of stop bits to be used during transmission.

timeout:

Will automatically log out the user after a period of inactivity.

If hangup is also enabled and a modem attached, the modem will also be disconnected after a timeout.

tftp:

Enables the configuration of the following parameters which are used for in-band downloads.

file_name:

Sets the name of the file on the file server to be downloaded.

file_type:

Use to specify the file type to be downloaded. The file type may be either **flash** or **boot** code depending on the code you are upgrading.

This command is only available for token-ring management module in-band downloads. It is not an option for the Ethernet management module

server_ip_address:

Sets the IP address of the server host which contains the file to be downloaded.

trunk:

The following trunk parameters can be configured using this command:

ring_in/ring_out cable monitor:

Enables or disables cable monitor mode on the copper RI and RO ports for token-ring modules. If enabled and a cable fault is sensed, the RI or RO ports will *wrap* to keep the ring operational.

ring_in/ring_out mode:

Enables or disables the RI and RO ports on token-ring modules.

ring_in network_map:

Use this command to enable or disable the Network Map feature between copper RI ports on token-ring modules.

When two copper trunk ports are connected between two hubs, the network map must be set to *external* so that the cable monitor mode can exist between the hubs.

- **show:**

  This is basically just a *read-only* command which enables the user to view the configuration parameters associated with the hub such as individual modules, ports or trunks. Additionally you can view network, module, port statistics counters and the error log information.

  You can also view usage information about the network paths.

  Note that port statistics are only available with the advanced token-ring management module which, we did not have access to when writing this book.

- **telnet:**

  Use this command to remotely login to any other token-ring management module.

- **?:**

  The *?* command lists available command and parameter options. For example, `save ?` lists the valid completions for the save command.

A subset of these commands can be executed by the ordinary user:

- Clear
- Logout
- Monitor
- Ping
- Show

15.2 Non-SNMP Agent Module Management

Provided you have a least one SNMP-enabled management module, all the non-SNMP agent token-ring modules can be managed from AIX HMP/6000.

For information on the out-of-band management commands for these modules refer to the module documentation supplied with your 8250.

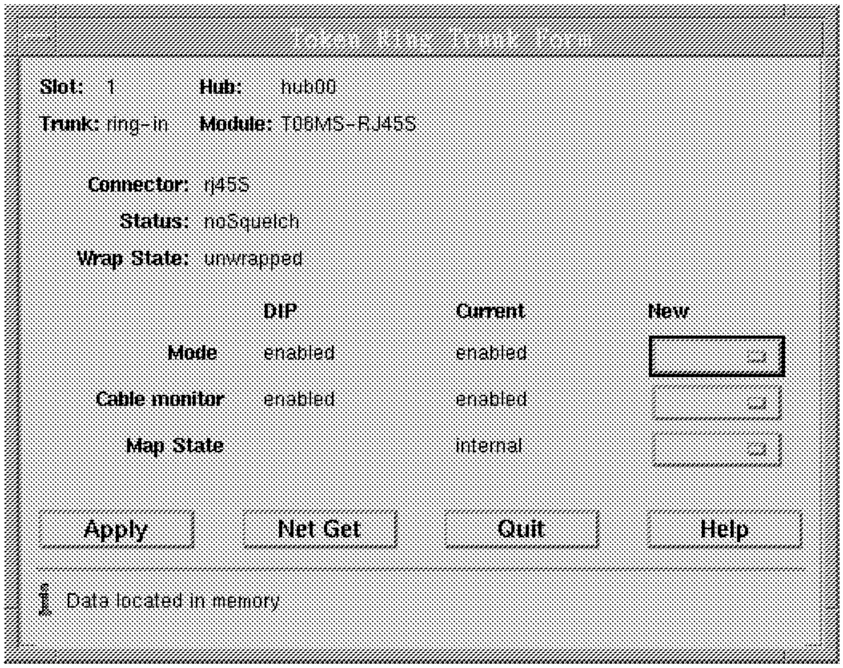
Issuing the equivalent in-band management commands from AIX HMP/6000 is relatively straight-forward. The forms corresponding to the module or port specific commands are invoked from the AIX HMP/6000 Hub Display window by clicking on the relevant module or port.

Below are some examples of these forms. We have not provided a complete list of possible forms as many of the differences are trivial.

15.2.1.1 An Example - The Token-Ring Twisted Pair MAU Module

The configuration form for this module allows you to change the module mode only. This is because of the fact that this module cannot be assigned to the backplane networks.

There are two separate port forms, one for the lobe ports and one for the RI/RO (trunk) ports. These are displayed by clicking on the corresponding port displays in the Hub Display window. Figure 173 on page 363 shows the *ring-in trunk form* for the MAU module.



Token-Ring Trunk Form

Slot: 1 **Hub:** hub00

Trunk: ring-in **Module:** T06MS-RJ45S

Connector: rj45S

Status: noSqueIch

Wrap State: unwrapped

	DIP	Current	New
Mode	enabled	enabled	
Cable monitor	enabled	enabled	
Map State		internal	

Data located in memory

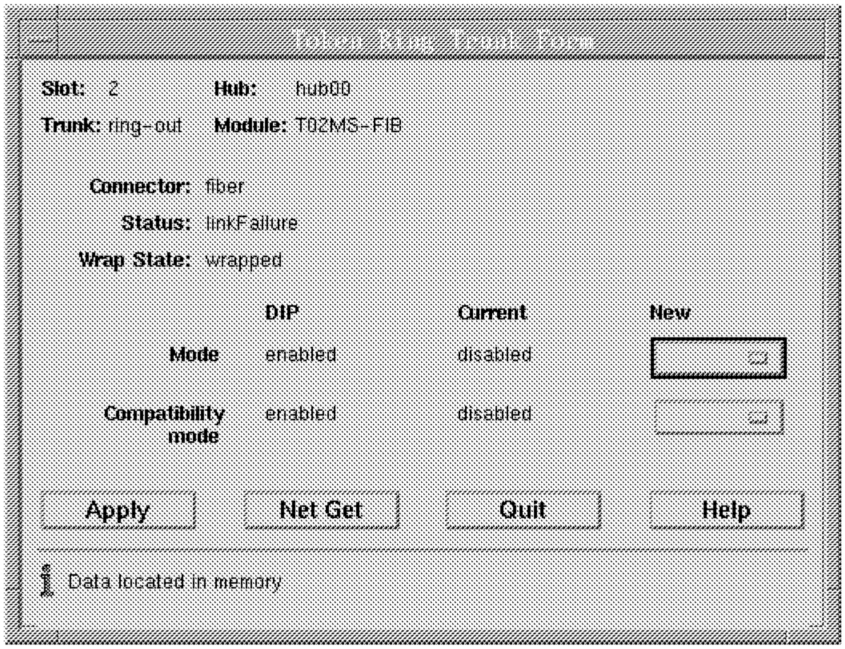
Figure 173. The Token-Ring Trunk Form. This is the trunk form for the ring-in trunk on the MAU module.

As can be seen in Figure 173, the *mode*, the *cable monitor* and the *map state* are all configurable for the ring-in/out trunks on the MAU module.

15.2.1.2 Another Example - The Token-Ring Fiber Repeater Module

The configuration form for this module allows you to set the network to which the module is attached and the ring speed.

There are three port forms, one for the fiber RI/RO (trunk), one for the copper RI/RO and one for the lobe ports. These are displayed by clicking on the corresponding port displays in the Hub Display window. Figure 174 on page 364 shows the Token-Ring Trunk Form for the fiber ring-out trunk.



Token Ring Trunk Form

Slot: 2 **Hub:** hub00

Trunk: ring-out **Module:** T02MS-FIB

Connector: fiber

Status: linkFailure

Wrap State: wrapped

	DIP	Current	New
Mode	enabled	disabled	
Compatibility mode	enabled	disabled	

Data located in memory

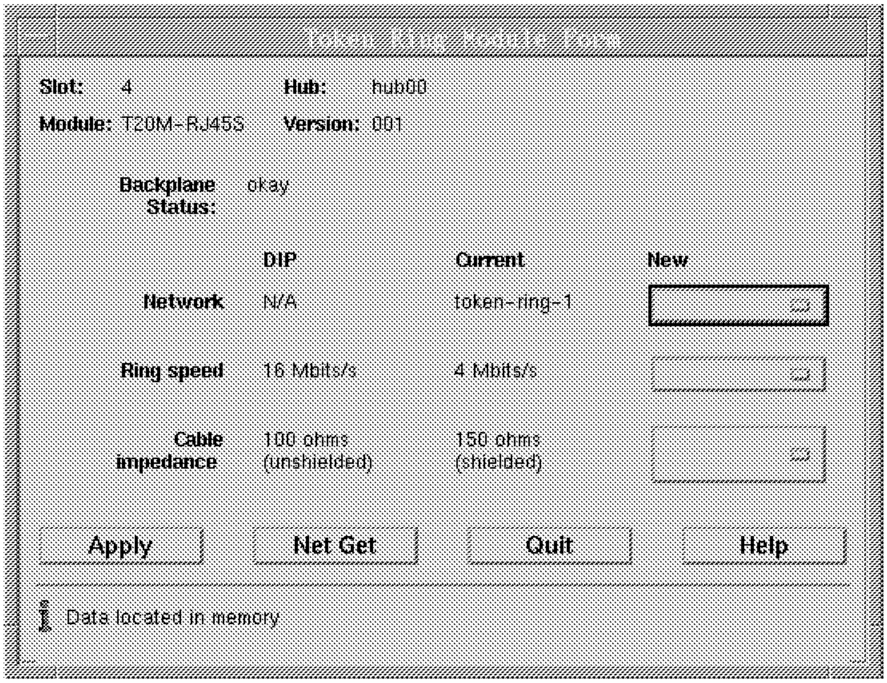
Figure 174. The Token-Ring Trunk Form. This is the trunk form for the ring-out trunk on the token-ring fiber repeater module.

From Figure 174 we see that the *mode* and the *compatibility mode* are the only configurable parameters for the ring-in/out trunks on the fiber repeater module.

15.2.1.3 A Final Example - The Token-Ring Twisted Pair Media Module

The configuration form for this module allows you to set the network to which the module is connected, the ring speed of the token-ring and the cable impedance for the whole module.

Figure 175 on page 365 shows the configuration form for this module.



Token Ring Module Form

Slot: 4 **Hub:** hub00

Module: T20M-RJ45S **Version:** 001

Backplane Status: okay

	DIP	Current	New
Network	N/A	token-ring-1	
Ring speed	16 Mbits/s	4 Mbits/s	
Cable impedance	100 ohms (unshielded)	150 ohms (shielded)	

Data located in memory

Figure 175. The Token-Ring Module Form. This is the configuration form for the token-ring twisted pair media module.

This module also supports a port-specific form, which allows you to set the characteristics of the individual ports.

15.3 Statistics Gathering

The statistics gathering function of AIX HMP/6000 is invoked from the *Tools* menu of the Hub Display window. This section defines the statistical information that can be gathered for token-ring networks and token-ring module ports.

There are 7 counters used in gathering token-ring statistics. They are outlined in Table 59.

Table 59 (Page 1 of 2). Token-Ring Traffic Statistics

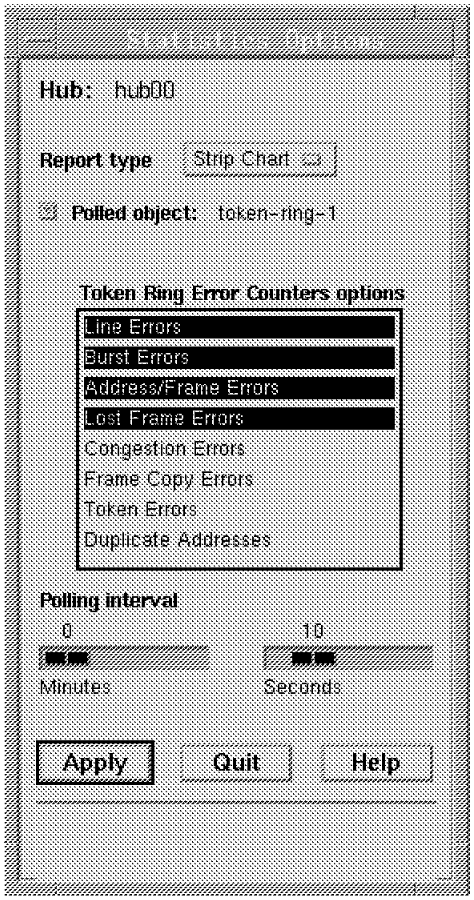
Counter Option	Description
Line Errors	The line error counter is incremented when: 1. A frame is repeated or copied, *and* 2. The *Error Detected* indicator in the incoming frame is zero, *and* 3. One of the following conditions exists: a. A code violation between the start and end frame delimiters b. A code violation in a token c. An FCS (Frame Check Sequence) error

Table 59 (Page 2 of 2). Token-Ring Traffic Statistics

Counter Option	Description
Burst Errors	The number of times a token-ring management module detects the absence of transitions for five half-bit times between the start and end delimiters or end and start delimiters.
Address/Frame Errors	The address/frame counter is incremented when a token-ring management module receives an AMP (Active Monitor Present) MAC frame with the address/frame bits equal to zero, *and* one or more SMP (Standby Monitor Present) MAC frames with the address/frame bits equal to zero, without receiving an intervening AMP MAC frame.
Lost Frame Errors	The number of times a token-ring management module is in transmit (stripping) mode and it fails to receive the end of the frame that it transmitted.
Receive Congestion Errors	The number of times an adapter in repeat mode recognizes a frame addressed to it but has no buffer space available to copy the frame.
Frame Copy Errors	The number of times an adapter in receive/repeat mode recognizes a frame addressed to it but finds the ARI bits not equal to zero. This indicates a possible line hit or duplicate address.
Token Errors	The token error counter is active only in the active monitor station. It is incremented when the active monitor detects an error with the token protocol according to one of the following conditions: 1. The monitor count bit of a token with a nonzero priority equals one. 2. The monitor count bit of a frame equals one. 3. No token or frame is received within a 10 ms time window. 4. The starting delimiter/token sequence has a code violation in an area where code violations must not exist.

15.3.1 An Example

From the **Tools** menu of the Hub Display window select **Statistics** to display the **Statistics Options** as shown in Figure 176 on page 367.



Hub: hub00

Report type: Strip Chart

Polled object: token-ring-1

Token Ring Error Counters options

- Line Errors (selected)
- Burst Errors (selected)
- Address/Frame Errors (selected)
- Lost Frame Errors (selected)
- Congestion Errors
- Frame Copy Errors
- Token Errors
- Duplicate Addresses

Polling interval

0 Minutes

10 Seconds

Figure 176. The Statistics Options Form. The options shown are consistent with the test case for this example.

This form allows you to set the type of output report, the network object to be analyzed, the parameters of that object to be gathered and the polling period which will be used to gather that information.

Using the **Report type** button we have selected a *Strip chart* report. For this example we have selected the *Line errors* counter, the *Burst errors* counter, the *Address/Frame errors* counter and the *Lost Frame errors* counter. These can be selected or de-selected simply by clicking on the corresponding counter option.

The **Polled object** button enables you to select a network or a specific port to be monitored. In this example we chose to monitor the Token-ring-1 network.

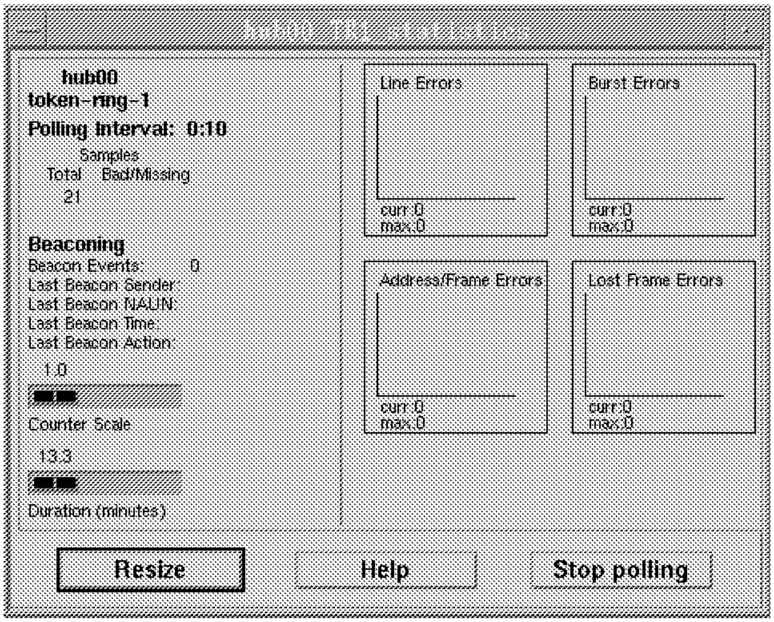
The **Polling interval** slide bar allows you to select the frequency of the test samples. There is a bar for both minutes and seconds. Five seconds is the minimum allowable test interval.

The **Statistical Option** form showing our selections is shown in Figure 176.

Note, if you select a large number of objects to be polled, AIX HMP/6000 may limit the display to prevent excessive system load.

Now, simply click on the Apply button to initiate the polling.

The results of this example do not show any output because the network was operating normally and the token-ring statistics counters are all related to errors.



hub00 TR1 statistics

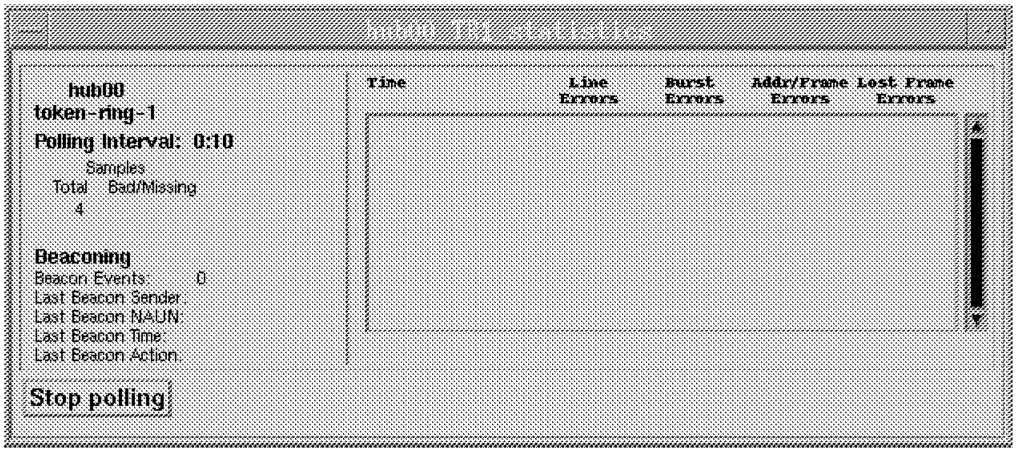
hub00
token-ring-1
Polling Interval: 0:10

Samples
Total Bad/Missing
21

Beaconing
Beacon Events: 0
Last Beacon Sender:
Last Beacon NAUN:
Last Beacon Time:
Last Beacon Action:

Figure 177. A Token-Ring Statistics Strip Chart Report

As a comparison we have shown the equivalent log report for the same test case in Figure 178. To get this output simply change the *Report type* parameter on the Statistics Option form to *Log report*.



hub00 TR1 statistics

hub00
token-ring-1
Polling Interval: 0:10

Samples
Total Bad/Missing
4

Beaconing
Beacon Events: 0
Last Beacon Sender:
Last Beacon NAUN:
Last Beacon Time:
Last Beacon Action:

Time	Line Errors	Burst Errors	Addr/Frame Errors	Lost Frame Errors

Figure 178. A Token-Ring Statistics Log Report

For both report types the output samples commence at the end of the first polling interval.

In addition to the options you select from the Statistics Options form, the following information is also displayed:

- **Beacon Events:**

  The number of beacon frames received.

- **Last Beacon Sender:**

  The address of the node from which the most recent beacon frame was received.

- **Last Beacon NAUN:**

  The Nearest Active Upstream Neighbor of the last station that transmitted a beacon frame.

- **Last Beacon Time:**

  The time that the most recent beacon frame was received.

- **Last Beacon Action:**

  The action taken when the last beacon frame received.

15.4 Access and Security

There are two levels of network security for the 8250 token-ring environment:

- Password security
- Address-to-port security

15.4.1 Password Security

There are two levels of password security that may be set for the token-ring management module:

Administrator Password: The administrator password provides both read and write access to all the commands. Use the following command to set the administrator password:

```
set device password administrator
```

User Password: The user password provides access to read-only commands. Use the following command to set the user password:

```
set device password user
```

For obvious security reasons the actual password is not echoed to the console when entered.

All passwords may contain up to 15 alphanumeric characters and are effective immediately though you must also issue the `save device` command for the new password to be permanently saved.

The password must be entered at the *Password:* prompt within 10 seconds or the terminal will timeout. If this happens, pressing the *Enter* key will re-display the prompt.

To discourage password guessing, after three invalid attempts, the console *sleeps* for thirty seconds before allowing another attempt.

15.4.2 Address-to-Port Security

The address-to-port security feature enables the token-ring management module to assign a known MAC address to a specific port and to detect when an unauthorized MAC address attempts to connect to the network via that port.

If a MAC address change is detected for a secure port, the token-ring management module will send an alarm to the token-ring management module console and disable the port.

To set port security, you must first define the address-to-port mapping for each token-ring port you wish to secure. For example:

```
set security port 4.17 mac_address 08-E2-0F-00-CC-CA
```

Having done this you then must enable the port security feature for those ports. This may be done on an individual port basis or for an entire module. For example, to enable security for port 17 in slot 4:

```
set security port 4.17 mode enable
```

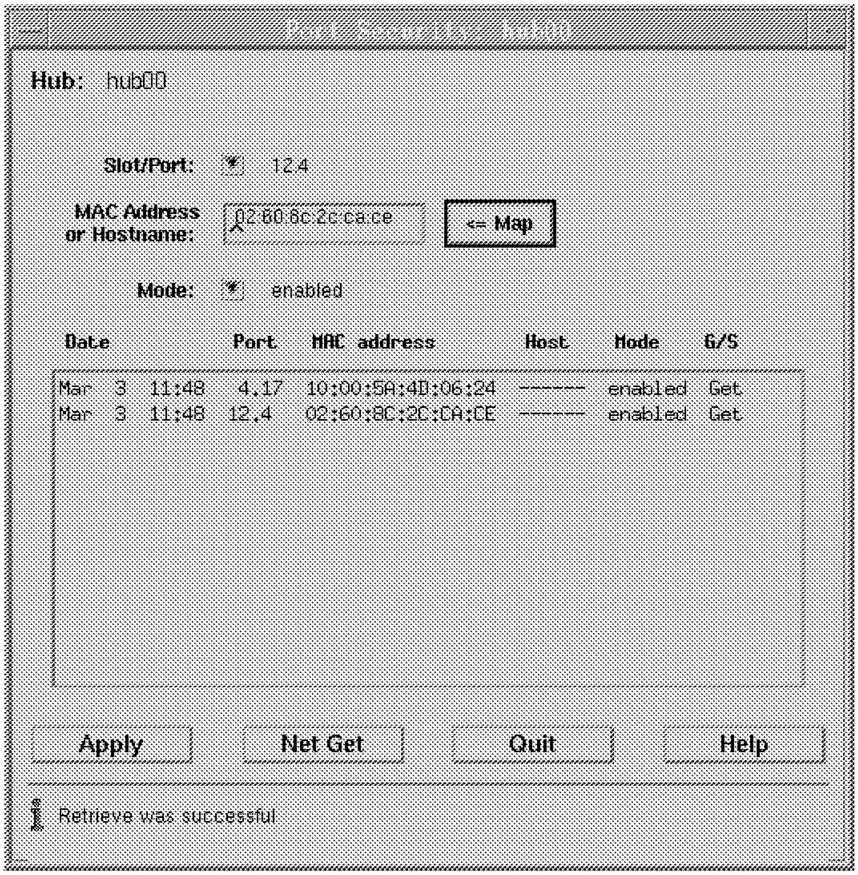
The same command can be used to *disable* port security.

More than one address can be assigned per port. In fact, a total of 1024 addresses per token-ring management module may be assigned to ports within a single 8250 hub.

A token-ring management module can be used to set port security for any token-ring port within an 8250, even those on token-ring networks to which the token-ring management module is not attached. A token-ring management module however, cannot be used to set security for Ethernet ports.

15.4.2.1 In-Band Port Security

Selecting the **Port Security** option from the *Tools* menu displays a form similar to the one shown in Figure 179 on page 371.



Hub: hub00

Slot/Port: 12.4

MAC Address or Hostname: 02:60:8c:2c:ca:ce

Mode: enabled

```
Date            Port   MAC address          Host     Mode     G/S
Mar  3  11:48    4.17  10:00:5A:4D:06:24    ------   enabled  Get
Mar  3  11:48   12.4   02:60:8C:2C:CA:CE    ------   enabled  Get
```

Retrieve was successful

Figure 179. Port Security Form

This form allows you to use AIX HMP/6000 to view or update port security information for any port on a specific module.

The **Slot/Port** parameter allows you to select a specific port on a specific module. When selected, this parameter will only display module/port options which are valid for the port security operation.

The **Map** button retrieves the MAC address of the device attached to the port.

The **Mode** field allows you to **enable** port security, **disable** port security, **clear** a previously assigned address for this port or perform **no change** when you only wish to view the results.

As can be seen in Figure 179, the port security form displays the following:

- **Date:**

  The date and time of the last operation on the port.

- **Port:**

  A fully qualified slot and port address.

- **MAC address:**

  The MAC address of a device assigned to the port.

- **Host:**

The host name of the device attached to the port.

- **Mode:**

  The selected operation performed on the port.

- **G/S:**

  Specifies whether the activity was the result of an SNMP Get or Set operation.

Index

ITSO Technical Bulletin Evaluation RED000

IBM 8250 Intelligent Hub and
IBM Hub Management Program/6000

Publication No. GG24-4033-00

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.

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 985, Building 657
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape **Please do not staple** Fold and Tape

Printed in U.S.A.

GG24-4033-00