8239 Token-Ring Stackable Hub

Setup and User's Guide

GA27-4209-01

8239 Token-Ring Stackable Hub

Setup and User's Guide

GA27-4209-01

Note

Before using this document, read the general information under “Notices” on page ix.

Second Edition (September 1998)

This edition applies to the 8239 Token-Ring Stackable Hub and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

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

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Design and Information Development
Department CGF
P.O. Box 12195
Research Triangle Park, NC 27709-9990
U.S.A.

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

Contents

Figures

Notices

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

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

Safety Information

Read this important safety information before using the 8239.

Safety Information Booklet

 **Danger:** Before you begin to install this product, read the safety information in *Caution: Safety Information—Read This First*, SD21-0030. This booklet describes safe procedures for cabling and plugging in electrical equipment.

 **Gevaar:** Voordat u begint met de installatie van dit produkt, moet u eerst de veiligheidsinstructies lezen in de brochure *PAS OP! Veiligheidsinstructies—Lees dit eerst,* SD21-0030. Hierin wordt beschreven hoe u electrische apparatuur op een veilige manier moet bekabelen en aansluiten.

 **Danger:** Avant de procéder à l'installation de ce produit, lisez d'abord les consignes de sécurité dans la brochure *ATTENTION: Consignes de sécurité—A lire au préalable,* SD21-0030. Cette brochure décrit les procédures pour câbler et connecter les appareils électriques en toute sécurité.

 **Perigo:** Antes de começar a instalar este produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança—Leia Isto Primeiro,* SD21-0030. Esse folheto descreve procedimentos de segurança para a instalação de cabos e conexões em equipamentos elétricos.

危險：安裝本產品之前， 請先閱讀 "Caution: Safety Information--Read This First" SD21-0030 手冊中所提供的安全注意事項。 這本手冊將會說明使用電器設備的纜線及電源的安全程序。

Opasnost: Prije nego sto počnete sa instalacijom produkta, pročitajte naputak o pravilima o sigurnom rukovanju u Upozorenje: Pravila o sigurnom rukovanju - Prvo pročitaj ovo, SD21-0030. Ovaj privitak opisuje sigurnosne postupke za priključrivanje kabela i priključivanje na električno napajanje.

Upozornění: než zahájíte instalaci tohoto produktu, přečtěte si nejprve bezpečnostní informace v pokynech „Bezpečnostní informace“ č. 21-0030. Tato brožurka popisuje bezpečnostní opatření pro kabeláž a zapojení elektrického zařízení.

 **Fare!** Før du installerer dette produkt, skal du læse sikkerhedsforskrifterne i *NB: Sikkerhedsforskrifter—Læs dette først* SD21-0030. Vejledningen beskriver den fremgangsmåde, du skal bruge ved tilslutning af kabler og udstyr.

 **Gevaar** Voordat u begint met het installeren van dit produkt, dient u eerst de veiligheidsrichtlijnen te lezen die zijn vermeld in de publikatie *Caution: Safety Information - Read This First*, SD21-0030. In dit boekje vindt u veilige procedures voor het aansluiten van elektrische appratuur.

 **VAARA:** Ennen kuin aloitat tämän tuotteen asennuksen, lue julkaisussa *Varoitus: Turvaohjeet—Lue tämä ensin*, SD21-0030, olevat turvaohjeet. Tässä kirjasessa on ohjeet siitä, miten sähkölaitteet kaapeloidaan ja kytketään turvallisesti.

 **Danger :** Avant d'installer le présent produit, consultez le livret *Attention : Informations pour la sécurité — Lisez-moi d'abord*, SD21-0030, qui décrit les procédures à respecter pour effectuer les opérations de câblage et brancher les équipements électriques en toute sécurité.

 **Vorsicht:** Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen—Bitte zuerst lesen,* IBM Form SD21-0030. Diese Veröffentlichung beschreibt die Sicherheitsvorkehrungen für das Verkabeln und Anschließen elektrischer Geräte.

Κίνδυνος: Πριν ξεκινήσετε την εγκατάσταση αυτού του προϊόντος, διαβάστε τις πληροφορίες ασφάλειας στο φυλλάδιο *Caution: Safety Information-Read this first,* SD21-0030. Στο φυλλάδιο αυτό περιγράφονται οι ασφαλείς διαδικασίες για την καλωδίωση των ηλεκτρικών συσκευών και τη σύνδεσή τους στην πρίζα.

Vigyázat: Mielôtt megkezdi a berendezés üzembe helyezését, olvassa el a *Caution: Safety Information— Read This First,* SD21-0030 könyvecskében leírt biztonsági információkat. Ez a könyv leírja, milyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.

Pericolo: prima di iniziare l'installazione di questo prodotto, leggere le informazioni relative alla sicurezza riportate nell'opuscolo *Attenzione: Informazioni di sicurezza — Prime informazioni da leggere* in cui sono descritte le procedure per il cablaggio ed il collegamento di apparecchiature elettriche.

危険： 導入作業を開始する前に、安全に関する
小冊子SD21-0030 の「最初にお読みください」
(Read This First)の項をお読みください。
この小冊子は、電気機器の安全な配線と接続の
手順について説明しています。

위험: 이 제품을 설치하기 전에 반드시
"주의: 안전 정보-시작하기 전에"
(SD21-0030) 에 있는 안전 정보를
읽으십시오.

ОПАСНОСТ
Пред да почнете да го инсталирате овој продукт, прочитајте
ја информацијата за безбедност:
"Предупредување: Информација за безбедност: Прочитајте го
прво ова", SD21-0030.
Оваа брошура опишува безбедносни процедури за каблирање
и вклучување на електрична опрема.

Fare: Før du begynner å installere dette produktet, må du lese sikkerhetsinformasjonen i *Advarsel: Sikkerhetsinformasjon — Les dette først*, SD21-0030 som beskriver sikkerhetsrutinene for kabling og tilkobling av elektrisk utstyr.

Uwaga:
Przed rozpoczęciem instalacji produktu należy zapoznać się z instrukcją:
"Caution: Safety Information - Read This First", SD21-0030.
Zawiera ona warunki bezpieczeństwa przy podłączaniu do sieci elektrycznej
i eksploatacji.

Perigo: Antes de iniciar a instalação deste produto, leia as informações de segurança *Cuidado: Informações de Segurança — Leia Primeiro*, SD21-0030. Este documento descreve como efectuar, de um modo seguro, as ligações eléctricas dos equipamentos.

ОСТОРОЖНО: Прежде чем инсталлировать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочесть в первую очередь", SD21-0030. В этой брошюре описаны безопасные способы каблирования и подключения электрического оборудования.

Nebezpečenstvo: Pred inštaláciou výrobku si prečítajte bezpečnosté predpisy v
Výstraha: Bezpeč osté predpisy - Prečítaj ako prvé, SD21 0030. V tejto brožúrke sú opísané bezpečnosté postupy pre pripojenie elektrických zariadení.

Pozor: Preden zaènete z instalacijo tega produkta preberite poglavje: 'Opozorilo: Informacije o varnem rokovanju-preberi pred uporabo," SD21-0030. To poglavje opisuje pravilne postopke za kabliranje,

Peligro: Antes de empezar a instalar este producto, lea la información de seguridad en *Atención: Información de Seguridad — Lea Esto Primero,* SD21-0030. Este documento describe los procedimientos de seguridad para cablear y enchufar equipos eléctricos.

Varning — livsfara: Innan du börjar installera den här produkten bör du läsa säkerhetsinformationen i dokumentet *Varning: Säkerhetsföreskrifter— Läs detta först,* SD21-0030. Där beskrivs hur du på ett säkert sätt ansluter elektrisk utrustning.

危險：

開始安裝此產品之前，請先閱讀安全資訊。

注意：

請先閱讀 - 安全資訊 SD21-0030

此冊子說明插接電器設備之電纜線的安全程序。

Power Disconnection

Danger: The main power disconnect for this unit is the appliance inlet located on the back of the machine. Therefore, the machine should be installed in such a way that the appliance inlet can be accessed.

اقبإفي يجآ ب!احمنمعب("ق!ل ت"تف!لذ" ج(يحجل!احمنمعب("ق لحظ عإع!احمغ٩آف عغفي آلما!احمنمعب("ق
!احمإفغغ٥آاحمنخ!لمعـ"ب|احمإحمبمس+–بتمغ+!لمعـ"ب(قبغف–ت–ة")"احمغجغمم(؟؟آلما!احمنمعب("ق
(تعغحمف

Gevaar: De stroom van deze eenheid kan alleen worden uitgeschakeld via de aansluiting op de achterkant van de machine. U dient de machine daarom zodanig op te stellen dat de aansluiting op de achterkant goed toegankelijk is.

Perigo:

O desligamento da energia principal desta unidade é efetuado através do dispositivo de entrada, localizado na parte posterior da máquina. Portanto, a máquina deve ser instalada de tal modo que o dispositivo de entrada possa ser acessado.

Opasnost:

Kod ovog uređaja je glavna mrežna slopka ugrađena na stražnjem dijelu. Shodno tome, uređaj treba montirati tako da je pristup do stražnjeg dijela uvijek moguć!

Nebezpečí: Pro odpojení napájení slouží síťový přívod v zadní části zařízení, které musí být proto instalováno tak, aby byl přívod přístupný. Síťová zásuvka musí být umístěna v blízkosti zařízení a musí být dobře přístupná.

Fare! Netledningen, der sluttes til bag på maskinen, fungerer som hovedafbryder. Maskinen skal derfor installeres sådan, at der er fri adgang til netledningen.

Vaara:

Tämän yksikön päävirta katkaistaan irrottamalla koneen takaosassa sijaitseva verkkojohto. Tämän vuoksi kone tulee asentaa siten, että verkkojohdon luo on esteetön pääsy.

DANGER. Le dispositif permettant de couper l'alimentation principale de cette unité se situe à l'arrière de la machine. Ce dispositif doit donc être accessible.

Vorsicht: Der Hauptschalter zur Unterbrechung der Stromversorgung für diese Einheit ist der Schalter, der sich auf der Rückseite der Maschine befindet. Die Maschine sollte daher so aufgestellt werden, daß dieser Schalter jederzeit zugänglich ist.

Κίνδυνος: Η αποσύνδεση της παροχής ρεύματος στη συσκευή γίνεται από την υποδοχή που βρίσκεται στο πίσω μέρος της μηχανής. Επομένως, η μηχανή πρέπει να εγκατασταθεί με τρόπο που να επιτρέπει την πρόσβαση στην υποδοχή αυτή.

Figyelem! A berendezés főkapcsolójának nyílása a hátoldalon található. A telepítést úgy kell elvégezni, hogy a főkapcsoló a későbbiekben is hozzáférhető legyen.

Pericolo: Per scollegare questa unità, occorre staccare la spina posta sul retro della macchina; pertanto la macchina deve essere installata in modo tale che tale spina sia accessibile.

危険：

この装置の非常時の電源の切断は機械の背面にある電源入力コネクターで行います。従って、装置を設置する場合はこのコネクターへのアクセスに障害のないようにしてください。

위험:

본체의 주 전원 차단을 위한 장치 삽입구가 뒷면에 있으므로 장치 삽입구를 쉽게 접근할 수 있도록 설치하여야 합니다.

Опасност:

Главното одвојување на електричното напојување за оваа единица е преку приклучокот од апаратот лоциран на задната страна од машината. Затоа, машината треба да биде инсталирана на таков начин за да може приклучокот од апаратот да биде пристапен.

Fare: Denne enheten frakobles hovednettet via apparatinntaket på baksiden av maskinen. Derfor må maskinen installeres slik at apparatinntaket er lett tilgjengelig.

Niebezpieczeństwo:

Główny wyłącznik sieciowy tej jednostki umieszczony jest we wnęce z tyłu urządzenia. Urządzenie powinno być ustawione w ten sposób, aby wyłącznik był łatwo dostępny.

Perigo: Para desligar a alimentação principal desta unidade é necessário desconectar o cabo da tomada eléctrica localizada na parte posterior da máquina. Por consequência, a máquina deve ser instalada de modo a permitir o fácil acesso a essa tomada.

ОПАСНО: Разъем для отключения питания данного блока расположен на задней стенке. Поэтому устанавливайте машину так, чтобы разъем питания был доступен.

危险：

切断本单元主要电源的设备入口位于机器后面。因此，机器的安装应便于接触设备入口。

Nebezpečenstvo

Hlavný prívod pre elektrinu sa nachádza na zadnej strane stroja. Z tohto dôvodu by mal byť stroj umiestnený tak, aby mohol byť tento prívod ľahko dostupný.

Nevarnost:

Kot glavni odklop napetosti za to enoto rabi vtičnica na zadnji strani stroja. Zato je treba stroj namestiti tako, da bo zagotovljen dostop do vtičnice.

Peligro: El interruptor principal de desconexión de esta unidad es la entrada de conexión del aparato situado en la parte trasera de la máquina. Por lo tanto, la máquina debe instalarse de modo que la entrada de conexión del aparato sea accesible.

FARA: Brytning av huvudströmmen till den här enheten görs vid elanslutningen på baksidan av maskinen. Placera därför maskinen så att elanslutningen är lättåtkomlig.

危險：本機器的主電源插頭在機器背面。安裝本機器時，請預留空間以方便連接或切斷電源。

Tehlike: Bu birimin elektrik bağlantısı, makinenin arkasındaki aygıt girişinden kesilir. Bu nedenle makine, arkasındaki aygıt girişine kolayca ulaşılabilecek biçimde kurulmalıdır.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1)this device may not cause harmful interference, and (2)this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes d'Industrie Canada

Cet appareil numérique de la classe A est conform à la norme NBM-003 du Canada.

European Community (CE) Mark of Conformity Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards. This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

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

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richlinie 89/336).

Dieses Gerät ist berechtigt in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland Informationssysteme GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.”

EN 50082-1 Hinweis: “Wird dieses Gerät in einer industriellen Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu vergrößern.”

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den IBM Handbüchern angegeben, zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) Statement

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Technology Equipment (VCCI). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Class A Warning Statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Battery Disposal

The 8239 Model 1 contains a clock module that has an embedded lithium battery. This battery is not replaceable. Please dispose of this module in accordance with local ordinances.

Trademarks

IBM and Nways are trademarks of the IBM Corporation in the United States or other countries or both.

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

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This manual contains information for anyone who is planning to install, configure, or manage an 8239 Token-Ring Stackable Hub (8239).

How This Manual Is Organized

This manual contains the following sections:

- Chapter 1, “Introduction and Planning” on page 1-1 introduces the functions, models, and physical requirements. It also contains configuration and network planning information.
- Chapter 2, “Installing the 8239 Hardware” on page 2-1 gives instructions for setting up the 8239.
- Chapter 3, “Installing Features” on page 3-1 provides information needed to install the optional features.
- Chapter 4, “Configuration” on page 4-1 describes the configuration process.
- Chapter 5, “Problem Determination Procedures” on page 5-1 provides problem determination procedures and lists all error codes.
- Chapter 6, “Concentrator Functions” on page 6-1 describes the concentrator functions provided by the 8239.
- Chapter 7, “8239 Device Management” on page 7-1 explains how to implement management of the device.
- Chapter 8, “Network Management” on page 8-1 contains information about accessing network management data.
- Chapter 9, “Planning Charts” on page 9-1 contains charts to help with planning for cabling and configuration.
- Appendix A, “Warranty Information” on page A-1 provides details about your warranty.

Related Publications

The following publications are shipped with the product in displayable softcopy form on the 8239 Token-Ring Stackable Hub Softcopy Library CD-ROM (08L3308):

8239 Token-Ring Stackable Hub Setup and User’s Guide, GA27-4209
8239 Token-Ring Stackable Hub Command Reference, GA27-4208

This CD-ROM is shipped with initial orders for the 8239.

These additional publications are shipped in hard copy:

- *8239 Token-Ring Stackable Hub Quick Reference,* GX27-4047
- *Caution: Safety Information - Read This First,* SD21-0030
- *License Agreement for Machine Code*, Z125-5468

Retrieve the latest 8239 MIB or 8239 operational code from our web site at:

`http://www.networking.ibm.com/support/8239`

For general information about token-ring architecture, see *Token-Ring Network Architecture*, SC30–3374.

Visit our Web Site

This IBM web page provides product information:

`http://www.networking.ibm.com/support/8239`

Chapter 1. Introduction and Planning

This chapter describes the functions of and the physical requirements for the IBM 8239 Token-Ring Stackable Hub (8239). It also contains planning information.

The 8239 is a stackable concentrator, allowing token-ring stations to share a network. Up to eight 8239s can be interconnected to form a stack. The stack connection provides a control path as well as a token-ring data path. The control path is an internal token-ring segment used by the stack units to communicate with each other. The token-ring data path connects the stack units into a shared token-ring network for user traffic. The 8239 is available in two models and provides a range of network management functions.

Models

Both models of the 8239:

- Support basic concentrator functions, such as attachment of port stations, beacon recovery, and address-to-port mapping.
- Attach up to 16 workstations
- Allow you to attach up to 32 workstations with an optional port expansion feature
- Provide configuration and status information for each device through an out-of-band connection

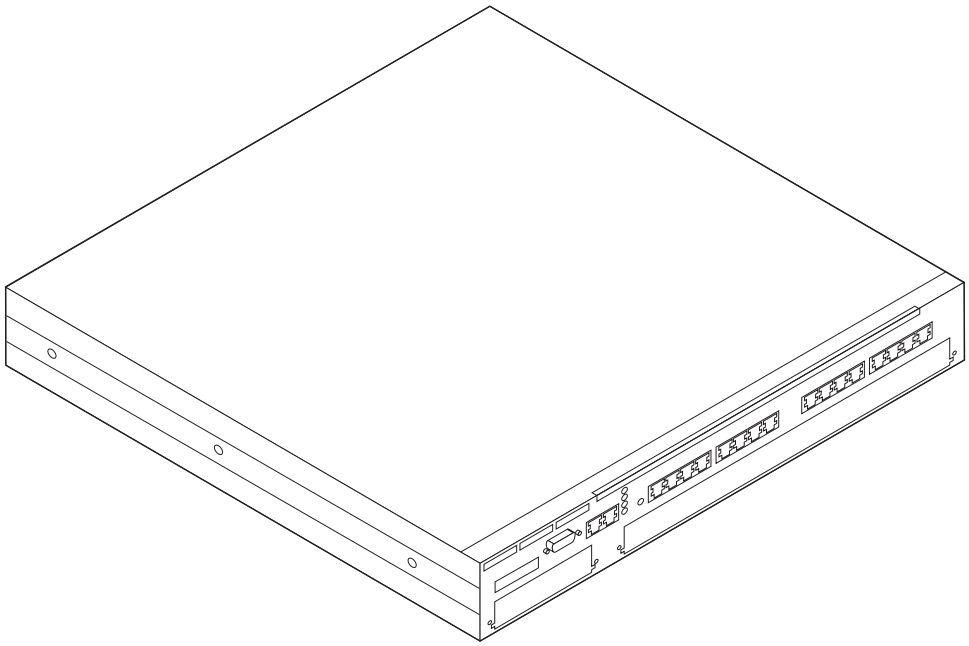

Figure 1-1. 8239 Model 1

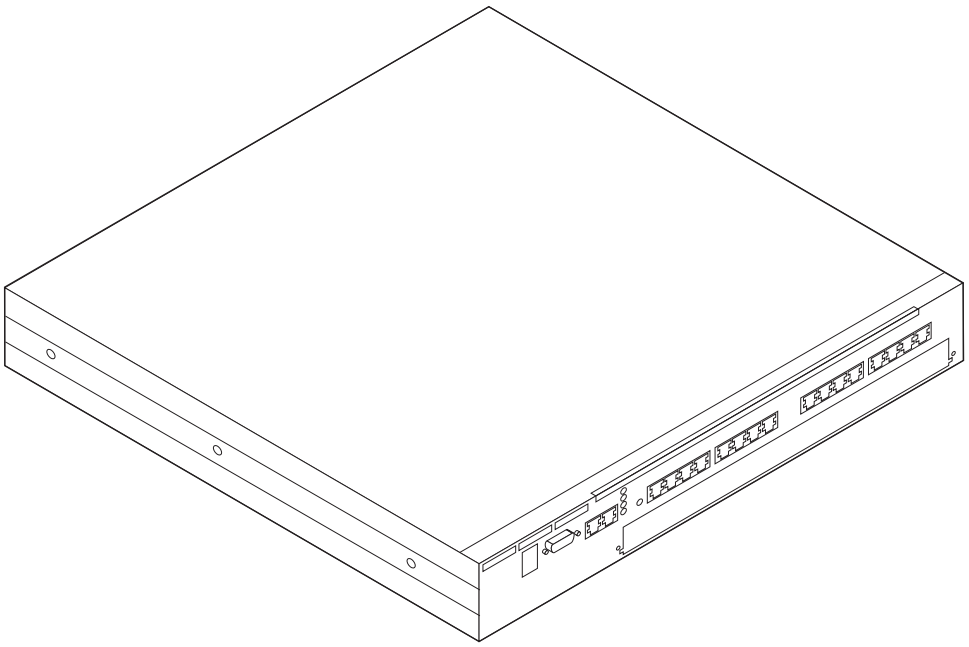

Figure 1-2. 8239 Model 2

The Model 1, in addition:

- Supports additional concentrator functions
- Provides network management functions
- Supports in-band connectivity
- Supports connection to other compatible concentrators

Features

The following optional features are available for the 8239.

- 16-Port Expansion Adapter

  The 16-Port Expansion Adapter contains 16 RJ-45 token-ring ports, increasing the supported number of ports in a single 8239 from 16 to 32. The 16-Port Expansion Adapter can be installed in the feature slot of the 8239.

- RI/RO Module (Model 1 only)

  Use the Ring In/Ring Out Module (RI/RO Module) to connect to another 8239 stack or to other compatible concentrators, such as:

  – Token-Ring 8228 Multistation Access Unit
  – 8230 Token-Ring Network Controlled Access Unit
  – 8238 Token-Ring Stackable Hub
  – 8260 Nways Multiprotocol Switching Hub

  It is installed in the RI/RO Module slot on the Model 1. There are two types of RI/RO Module:

  – RJ-45 RI/RO Module, providing an RJ-45 copper interface

  – Optical Fiber RI/RO Module, providing an ST-connector optical fiber interface

Configuration

The 8239 is shipped with a default configuration. If this configuration is acceptable, you need only power on the 8239 and connect the cables. The configuration parameters along with their default values are listed in “Configuration Parameters” on page 4-9.

If you need to change the configuration, you can do so using:

- EIA-232 terminal interface (both models)
- Telnet terminal interface (Model 1 only)
- SNMP (Model 1 only)
- BOOTP (Model 1 only)
- Configuration setup file loaded via XMODEM (both models) or TFTP (Model 1 only)

Concentrator Functions

Each 8239 provides 16 RJ-45 token-ring ports. Cabling may be either unshielded twisted pair (UTP) or shielded twisted pair (STP). The 8239 has an expansion slot that allows you to add 16 additional RJ-45 ports, for a total of 32 ports. Up to eight 8239 can be connected to form a single stack using the stack-in and stack-out ports. Thus, there can be up to 256 token-ring ports supported in an 8239 stack. Any combination of 8239 Model 1s and 8239 Model 2s can make up a stack.

The 8239 provides address-to-port mapping information that identifies which MAC addresses are attached to which ports on the 8239. Fanout devices and MAC-less devices attached to 8239 ports also are supported by this mapping feature.

The 8239 provides port security. Port security allows you to identify specific MAC addresses that are permitted to insert at a given port. You can configure a port to respond to a security intrusion by:

- Disabling the port
- Reporting the intrusion attempt
- Disabling and reporting the intrusion attempt

The 8239 provides automatic beacon recovery when hard-error faults occur. Hard-error faults are automatically detected and isolated to minimize the impact on the network.

Segmentation support in the 8239 lets you create smaller data segments within a stack and still use a single interface to manage the stack.

Device and Network Management

The 8239 can be managed in these ways:

- Out-of-band access through the EIA-232 port
- In-band access using Telnet, SNMP, PING, and TFTP (8239 Model 1 only)

Device management consists of configuring the stack, obtaining status information from the stack, and loading code on the stack.

The network management functions supported by the 8239 Model 1 are:

- IEEE 802.5 Token Ring MIB
- MIB II
- Remote Monitoring (RMON)
- RMON 2
- Enterprise Communications Analysis Module (ECAM)
- IBM Token Ring Surrogate MIB and Surrogate Trap MIB

Network management for the 8239 is provided by the following Nways Network Management products:

For graphical device (element) management

- IBM Nways Workgroup Manager for Windows NT Version 1.1.2 or later
- IBM Nways Manager for AIX Version 1.2.2 or later — Campus Manager LAN component
- IBM Nways Manager for HP-UX Version 1.2 or later — Element Manager component

For remote network monitoring (RMON/RMON2/ECAM)

- IBM Nways Workgroup Remote Monitor for Windows NT Version 1.1 or later
- IBM Nways Manager for AIX Version 1.2 or later — Remote Monitor and Traffic Monitor components
- IBM Nways Manager for HP-UX Version 1.2 or later — Remote Monitor component

For media management using the IBM Token Ring Surrogate MIB

- IBM Nways Manager for AIX Version 1.2.2 or later — Campus Manager LAN component

The 8239 fully supports RMON, RMON 2 and ECAM. However, the versions of remote network monitoring applications mentioned above have varying levels of RMON, RMON 2, or ECAM support.

Cable Types and Distances

This section gives information about supported cable types and maximum cable distances.

Ports

Table 1-1 shows the types of cable and maximum distances supported for port cabling.

Table 1-1. Port Cabling

Cable Type	4-Mbps Ring Speed	16-Mbps Ring Speed
UTP, ScTP, or FTP Cat 3	250 m (820 ft)	100 m (328 ft)
UTP, ScTP, or FTP Cat 4	425 m (1394 ft)	210 m (689 ft)
UTP, ScTP, or FTP Cat 5	425 m (1394 ft)	225 m (738 ft)
STP or STP-A	750 m (2460 ft)	375 m (1230 ft)

Stack Unit Cabling

You can install up to eight 8239s in a stack, using any combination of 8239 Model 1s and 8239 Model 2s in the stack. Use standard TIA/EIA/ANSI 568A or ISO/IEC 11801 Category 5 cable for your stack.

Determining Maximum Cable Length

Each of the 8239s in a stack can be up to 25m (82 ft) apart without regard to the total distance among all 8239s in the stack. If distances over 25m are required, they are supported provided that the sum of all of the stack cable lengths minus the length of the shortest stack cable does not exceed 210 M (689 ft). For example, four 8239s have the following stack cables connecting them to form a stack:

Cable 1 connects stack unit 1 to stack unit 2	1 m
Cable 2 connects stack unit 2 to stack unit 3	25 m
Cable 3 connects stack unit 3 to stack unit 4	25 m
Cable 4 connects stack unit 4 to stack unit 1	150 m

To see if this configuration is allowable, use this formula:

```
(Total length of stack cables) - (length of shortest cable) < 210 m
```

Substituting the values in the example in this formula:

```
1 + 25 + 25 + 150 - 1 = 200
```

Because 200 m is less than 210 m, this configuration is allowable. In this case, even though there are lengths of cable that are greater than 25 m, the configuration is still acceptable because the total distance is less than 210 m.

Attention: To prevent ring disruptions, be sure you connect Stack-In and Stack-Out cables at both ends.

RI/RO Module

This section describes cabling for the RJ-45 RI/RO Module and the Optical Fiber RI/RO Module.

RJ-45 RI/RO Module

Table 1-2 shows the types of cable and maximum distances supported for the RJ-45 RI/RO Module.

Table 1-2. RJ-45 RI/RO Module Cabling

Cable Type	4-Mbps Ring Speed	16-Mbps Ring Speed
UTP, ScTP, or FTP Cat 3	250 m (820 ft)	100 m (328 ft)
UTP, ScTP, or FTP Cat 4	425 m (1394 ft)	210 m (689 ft)
UTP, ScTP, or FTP Cat 5	425 m (1394 ft)	225 m (738 ft)
STP or STP-A	750 m (2460 ft)	375 m (1230 ft)

Optical Fiber RI/RO Module

The recommended maximum fiber length that can be used between Ring In and Ring Out fiber connections is 2 km (1.2 miles) of 62.5/125-micron multimode optical fiber cable. This distance applies to both 4-Mbps and 16-Mbps rings. See *IBM Cabling System Optical Fiber Planning and Installation*, GA27–3943, for more information about optical fiber.

Physical Specifications

This section gives the physical specifications, environmental requirements, and power requirements of the 8239.

Dimensions

Figure 1-3 shows the exterior dimensions of the 8239.

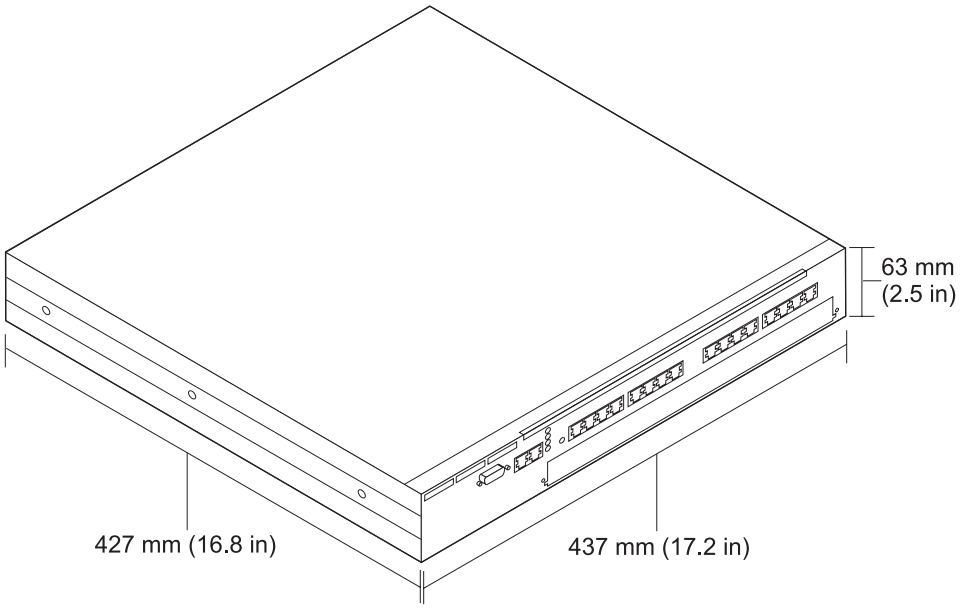

Figure 1-3. 8239 Dimensions

Placement

The 8239 can be placed on a tabletop or installed in a customer-supplied rack.

To surface-mount the 8239, choose a flat horizontal surface sturdy enough to support the weight of the 8239. Do not mount the 8239 vertically.

The 8239 can be installed in a standard, open, EIA 19-in. rack in a wiring-closet environment. The rack must meet the requirements of ANSI/EIA RS-310-C. The 8239 requires 1.5 rack units.

Weight

8239 Model 1: 7.0 kg (15.4 lb) when empty; 7.4 kg (16.4 lb) when fully loaded

8239 Model 2: 7.0 kg (15.4 lb) when empty; 7.4 kg (16.2 lb) when fully loaded

Service Clearances

Front	Adequate space to view LEDs
Sides	Minimum of 50 mm (2 in.) for cooling purposes
Rear	Minimum of 130 mm (5 in.) to provide for cables

Environmental Requirements

Operating Temperature	10°— 40° C (50°—104° F)
Storage Temperature	-40°—60° C (-40°—140° F)
Humidity	20°—85%

Power Requirements

The 8239 requires input ac voltage within the range of 88 V ac to 265 V ac at a frequency of 47 Hz to 63 Hz.

The maximum power consumption of an 8239 that is fully populated with features is 85 W.

Chapter 2. Installing the 8239 Hardware

This chapter provides instructions for setting up the 8239.

Before installing the 8239, be sure to read “Safety Information” on page ix.

Preparing for Setup

Complete the following tasks before beginning the setup process:

- Verify that appropriate power outlets are available.
- Gather network documentation identifying devices and specifying port connections. The network administrator is responsible for network planning. Worksheets for planning your 8239 installation are provided in Chapter 9, “Planning Charts” on page 9-1.
- You will need access to a local ASCII terminal or to the terminal that is being used for remote access.

Verifying the Shipment

After you have unpacked the shipping container, use the following Inventory Checklist to verify that you have the items listed.

Inventory Checklist

- Hardware

  __ 8239 Model 1 or Model 2
  __ Power cord (U.S., Canada, and Latin America)
  __ Stack Cable (standard Category 5 UTP)
  __ Cable management bracket

- Media

  __CD containing this information:

  8239 Token-Ring Stackable Hub Setup and User’s Guide (this book)
  8239 Token-Ring Stackable Hub Command Reference

- Printed publications

  __ *License Agreement for Machine Code*
  __ *8239 Token-Ring Stackable Hub Quick Reference*
  __ *Caution: Safety Information - Read This First*
  __ *Network Management* trial offer
  __ *Release Notes*

Note: Download the latest IBM 8239 MIB from this IBM web site: *http://www.networking.ibm.com/support/8239*.

Installing Features

The following features may be installed in the 8239:

- Optical Fiber RI/RO Module (Model 1 only)
- RJ-45 RI/RO Module (Model 1 only)
- 16-Port Expansion Adapter

For instructions for the installation of these features, go to Chapter 3, Installing Features.

Placing the 8239

The 8239 can be placed on a tabletop or installed in a customer-supplied rack.

If you are installing this 8239 in a rack, go to “Rack-Mounting the 8239.” Otherwise, continue with “Surface-Mounting the 8239.”

Surface-Mounting the 8239

Place the 8239 on a flat horizontal surface sturdy enough to support its weight. The 8239 is not designed for vertical mounting.

Continue with “Connecting the Cables” on page 2-4.

Rack-Mounting the 8239

The 8239 can be installed in a standard, open, EIA 19–in. rack in a wiring-closet environment.

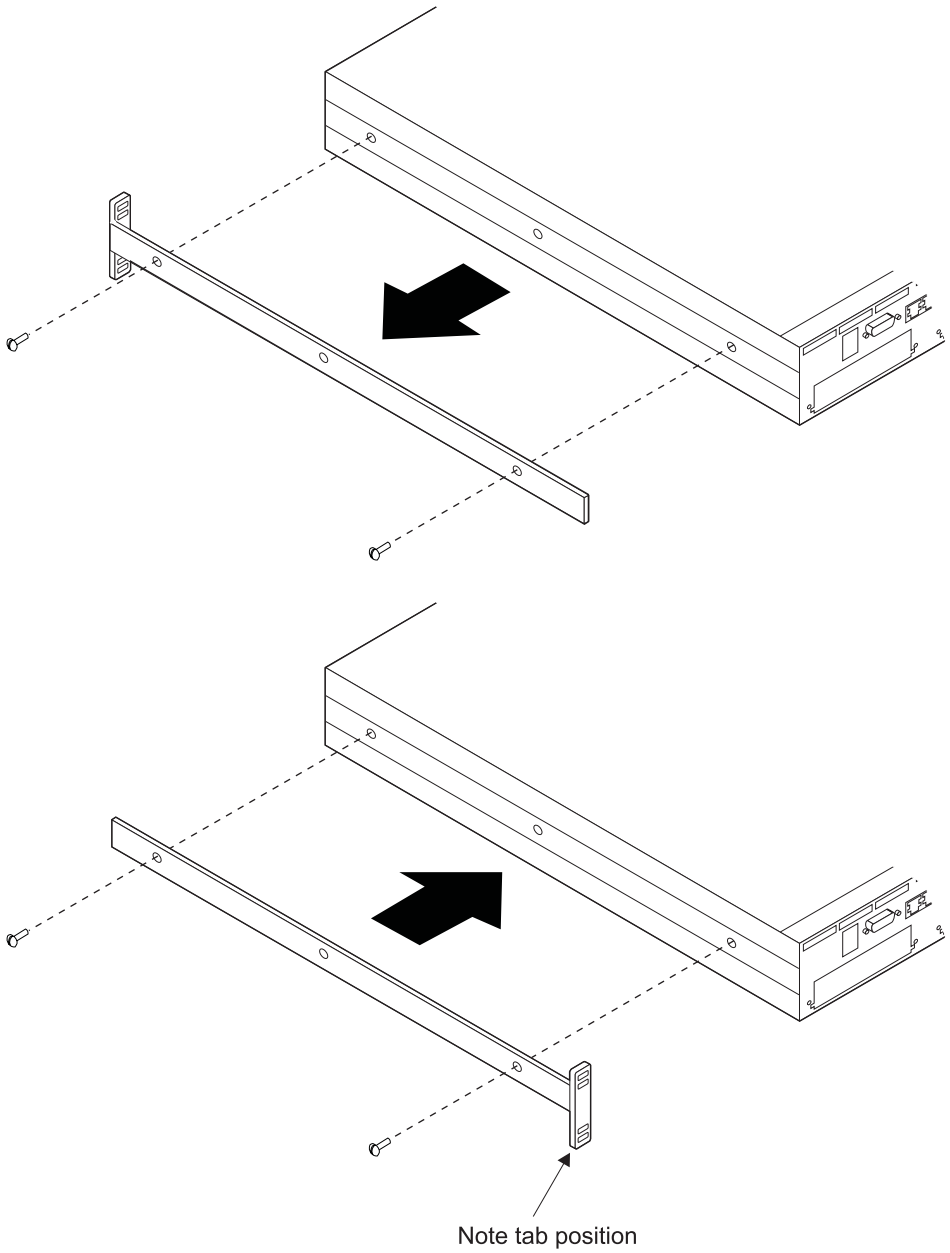

Figure 2-1. Rotating the Rack-Mounting Brackets

1. Using a Phillips screwdriver, remove the four screws, two on each side, that attach the mounting brackets to the sides of the 8239, as shown in Figure 2-1.
2. Rotate the brackets and reattach them.
3. Refer to your network documentation to determine where in the rack to mount the 8239.
4. Gather the rack-mounting screws (not provided) and place them within reach.
5. Hold the 8239 in position in the rack and start the lower of the two screws that will secure the left bracket.
6. On the right side, align the lower screw holes in the mounting bracket and the cable management bracket with the correct hole of the rack; then start the screw as shown in Figure 2-2 on page 2-4.

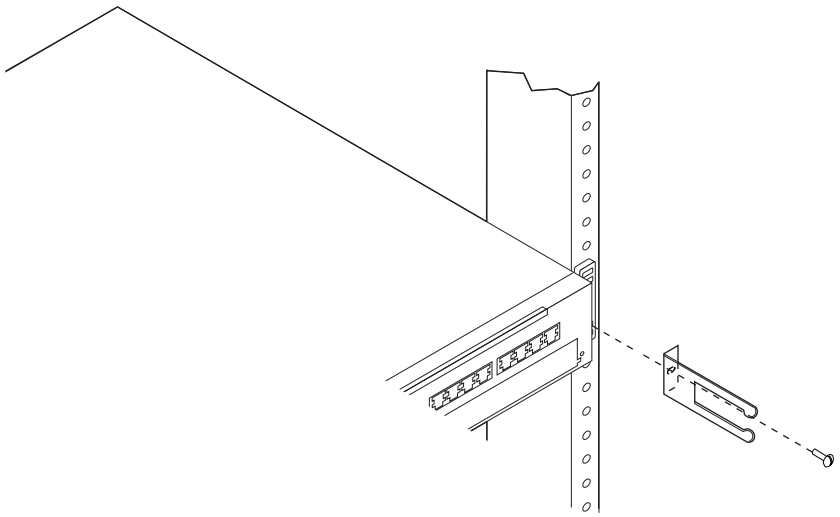

Figure 2-2. Attaching the Cable Management Bracket

7. Tighten the screws on each side.

Connecting the Cables

Use this section to connect cables to the 8239 and any attaching devices.

Connecting Stations to the 8239

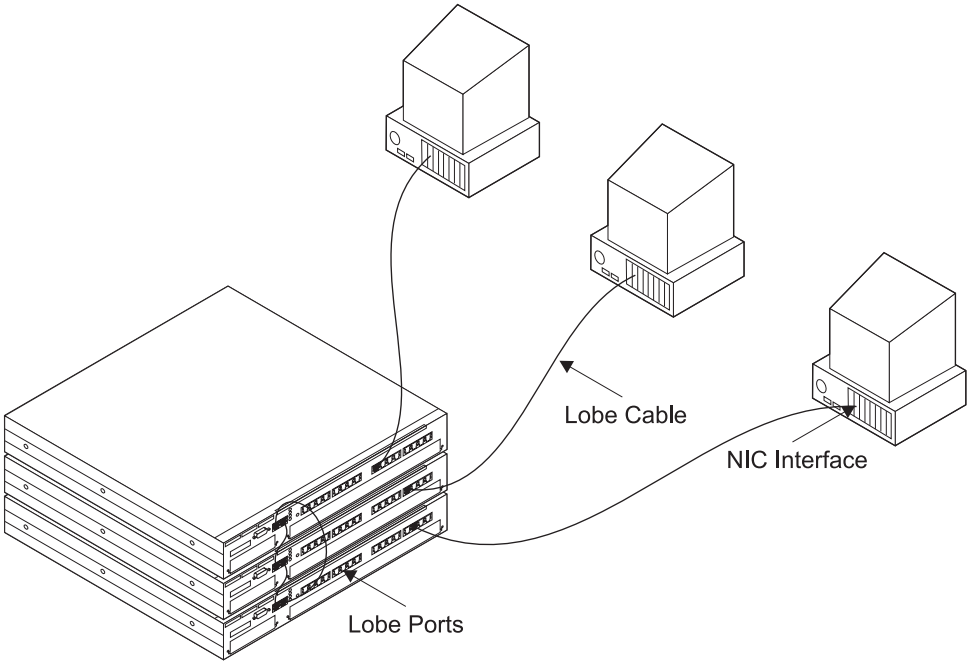

Figure 2-3. Connecting Stations to the 8239

1. Refer to your network documentation to determine each cable's port assignment.
2. Connect the lobe cable (not provided) to a lobe port on the 8239.

3. Label the cable at the lobe port with a unique identifier so that it will be easy to identify the location of the device at the other end of the cable should you have to troubleshoot a network problem.
4. Connect the other end of the cable to the end station faceplate or other intermediate connection point, as required.

   Label the cables at the attaching-device end.

Cabling a Stack

Note: The stack cable shipped with the 8239 Model 1 is longer than the cable shipped with the Model 2, providing the means to connect the top 8239 to the bottom 8239.

To build a hub stack containing two to eight 8239s:

1. Beginning with the 8239 at the top of the stack, use a stack cable to connect stack OUT on the top 8239 to stack IN on the next hub below in the stack.

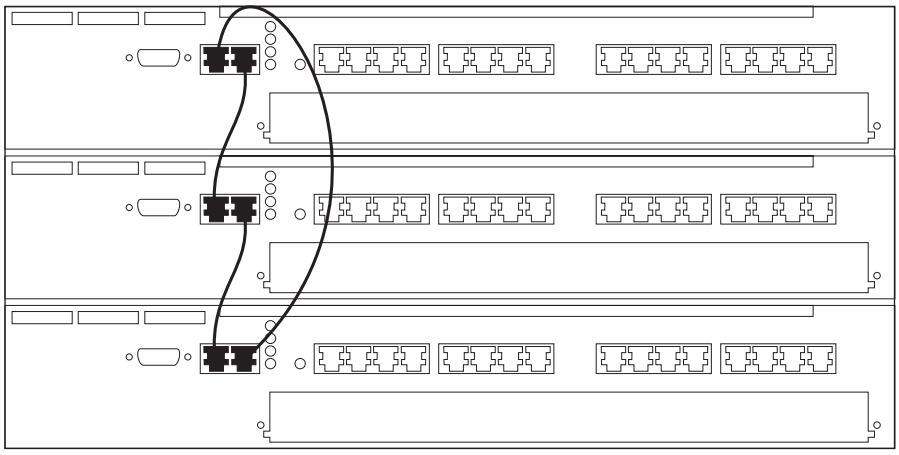

Figure 2-4. Stack Building

2. Using stack cables, continue to connect stack OUT on each 8239 to stack IN on the next 8239 in the stack.
3. Use the stack cable to connect stack IN on the top 8239 to stack OUT on the bottom 8239.

To prevent network disruptions, be sure you connect stack cables at both ends.

Connecting an ASCII Terminal or Modem to the EIA-232 Port

If you are going to access the 8239 without using the data network, you must attach either an ASCII terminal for local access to the 8239 or a modem for remote access.

ASCII Terminal

To attach an ASCII terminal, follow these steps:

1. Connect one end of the special null-modem cable (not provided) to the EIA-232 port of the 8239 that is going to be used.
2. Connect the other end of the cable to the communications port of your ASCII terminal

Modem

For general suggestions about using a modem with the 8239 Token-Ring Stackable Hub and setting information for specific modems, go to “Modem Connection” on page 2-7 before continuing.

To attach a modem, follow these steps:

1. Unpack the modem and install it according to the manufacturer’s instructions.
2. Connect one end of the standard modem DTE cable (not provided) to the EIA-232 port on the 8239.
3. Connect the other end of the cable to the modem.
4. Configure the modem to use the same settings as those on the 8239 you are using (refer to “Management Using Emulation Software” on page 4-1).
5. Place the modem in auto-answer mode.
6. Set up the remote modem and data terminal.
7. Establish a modem link as described in the modem user documentation.

Note: Configuration command syntax varies from modem to modem. Make sure that the modem has the following characteristics:

- asynchronous mode
- disable modem responses
- disable flow control (for example, AT \Q)
- disable echo (for example, AT Q1)
- auto-answer mode on second ring (for example, AT S0=2)

After configuring the modem, save its configuration.

Powering On the 8239

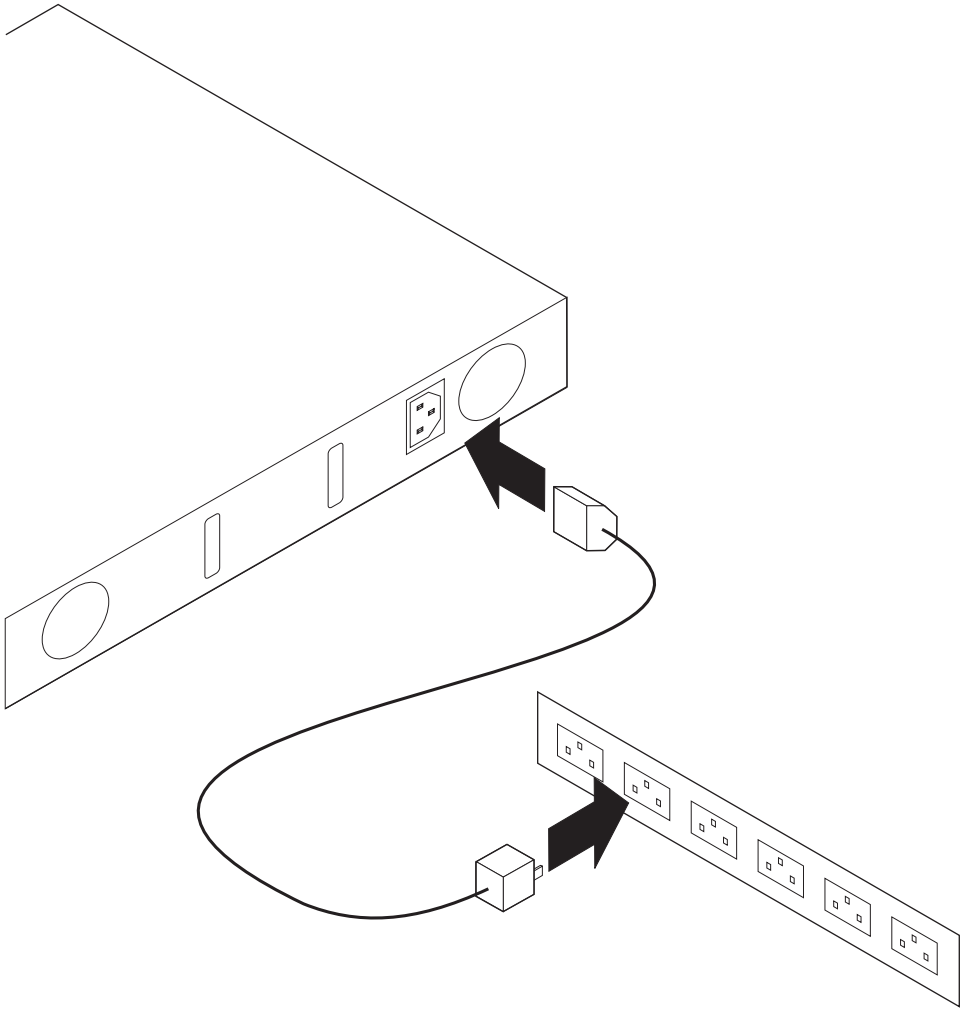

Figure 2-5. Power on the 8239

1. Connect the power cord to the connector at the rear of the 8239.
2. Plug the power cord into the power outlet.

Because the 8239 has no power switch, the power-on self-test (POST) begins as soon as you plug in the power cord. POST requires up to 2 minutes. At the end of POST, the LCD on the 8239 Model 1 shows the operational code version for about 5 seconds. A successful power-on is indicated when the green OK light-emitting diode (LED) is lit and the yellow OK LED is off.

Modem Connection

This section contains:

- General suggestions about using modems with the 8239 Token-Ring Stackable Hub
- Setting information for several specific modems

Modem Hints

- It is helpful to consider the modem as an extension of the EIA-232 terminal, rather than as a controller of the 8239. There are no *smart* requirements for interaction between the modem and the 8239. Such features can actually cause problems during the connection handshaking.
- Be sure to disable both software and hardware flow control. The 8239 will not try to communicate with the modem using any EIA-232 control lines, DTR, DSR, and so on; the modem should ignore these. Turning off all flow control is a one-step command with some modems, but with other modems, you may have to execute several commands to completely disable flow control.

Settings for Specific Modems

Sportster 14.4

Note that external switch settings take precedence over stored values after resetting the modem. Set the switches in this fashion, where *Down* = on:

1	Down
4	Down
8	Down
All others	Up

Use the following command string to set up the modem:

```
ATE0F1Q1&H0&R1S0=1
```

Be sure to save the results.

28.8 FaxModem V.34/V.32 bis

Note that external switch settings take precedence over stored values after resetting the modem.

Set the switches in this fashion, where *Down*=on:

1	Down
2	Down
4	Down
6	Down
8	Down
All others	Up

Use the following command string to set up the modem:

```
ATF1Q1&H0&R1S0=1
```

Be sure to save the results.

IBM 7855

Using the factory default settings, set up the modem with the following command:

```
ATE0Q1&D0\Q0\R0&S0S0=1
```

Be sure to save the results.

IBM 7858

Using the factory default settings, set up the modem with the following command:

```
ATE0Q1&D0&K0&U0S0=1
```

Be sure to save the results.

Chapter 3. Installing Features

16-Port Expansion Adapter

To install or remove a 16-Port Expansion Adapter, follow the directions in this section. The 16-Port Expansion Adapter is hot pluggable, so you do not need to disconnect the 8239 power cord.

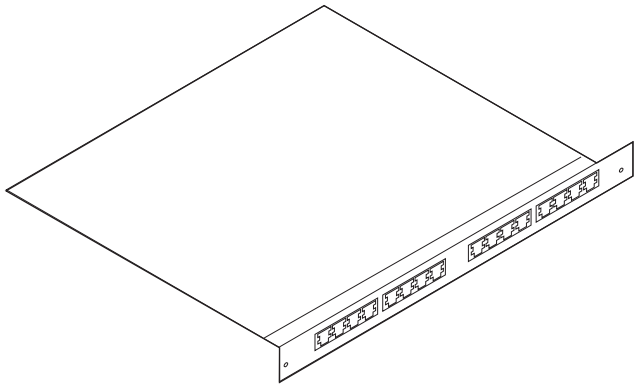

Figure 3-1. 16-Port Expansion Adapter

Removing a 16-Port Expansion Adapter

1. If you intend to replace the 16-Port Expansion Adapter, label the cables attached to it to ensure that you reconnect the cables correctly.
2. Disconnect the cables from the 16-Port Expansion Adapter.
3. Loosen the two thumbscrews by turning them counterclockwise until the screws are loose enough to remove the card from the 8239.
4. Remove the 16-Port Expansion Adapter from the 8239 by pulling on the thumb screws.
5. If you are not replacing the 16-Port Expansion Adapter immediately, install an expansion slot cover.

Installing a 16-Port Expansion Adapter

Perform these steps to install a 16-Port Expansion Adapter:

1. If a 16-Port Expansion Adapter was not already installed in this 8239, remove the slot cover and store it in a safe place.
2. Slide the 16-Port Expansion Adapter along the grooves in the slot until it is seated and flush with the front panel.
3. Tighten the thumbscrews by turning them clockwise.
4. After the adapter is seated, all of the yellow port LEDs are on briefly, indicating that diagnostic tests are in progress.
5. The diagnostic tests for the 16-Port Expansion Adapter will complete in less than 5 seconds.

6. Use the DISPLAY INVENTORY terminal interface command to verify that the 8239 recognizes the 16-Port Expansion Adapter.

RI/RO Module

To install or remove a Ring In/Ring Out Module, follow the directions in this section.

Attention: You must power off the 8239 before installing or removing a Ring In/Ring Out Module.

You do not need to remove the 8239 from a rack to remove or install a RI/RO Module.

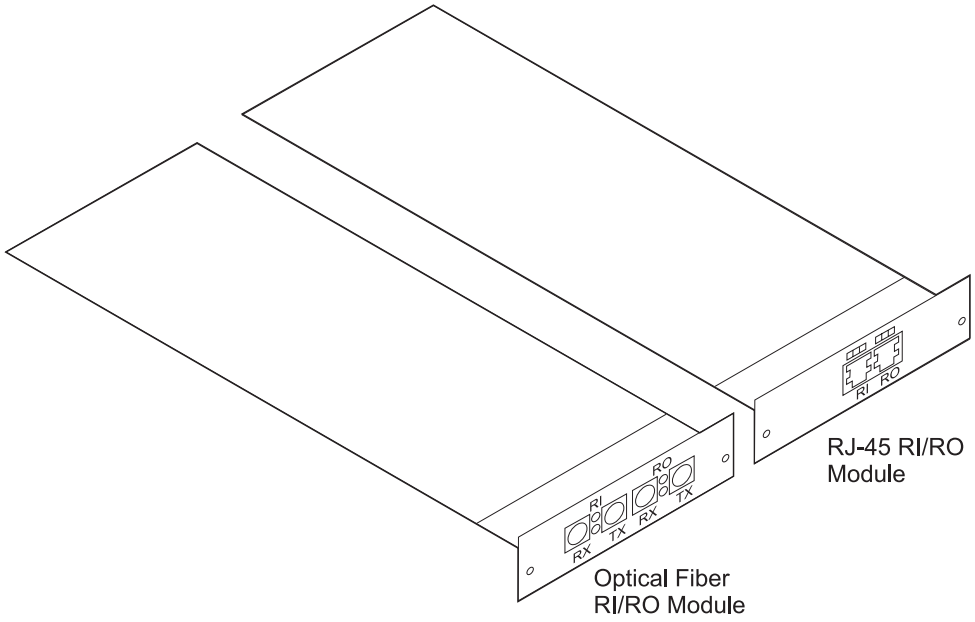

Figure 3-2. RI/RO Module

Removing a RI/RO Module

1. **Remove power from the 8239 by unplugging the power cord.**
2. If you intend to replace the RI/RO Module, label the cables attached to it. This precaution will ensure that you reconnect the cables correctly.
3. Disconnect the cables from the RI/RO Module.
4. Loosen the two thumbscrews by turning them counterclockwise until the screws are loose enough to remove the module from the 8239.
5. Pull the RI/RO Module along the grooves of the guide rail and remove it from the 8239.
6. If you are not replacing the RI/RO Module immediately, install a slot cover and provide power to the 8239.

Installing a RI/RO Module

Perform these steps to install a RI/RO Module:

1. **Remove power from the 8239 by unplugging the power cord.**
2. If a RI/RO Module was not already installed in this 8239, remove the slot cover and store it in a safe place.
3. Slide the module into the slot along the grooves of the guide rail until it is seated and flush with the front panel.
4. Tighten the thumbscrews by turning them clockwise.
5. Connect the cables connecting RI on the 8239 RI/RO Module to RO on the external device and RO on the 8239 RI/RO Module to RI on the external device.
   - For the Optical Fiber RI/RO Module:

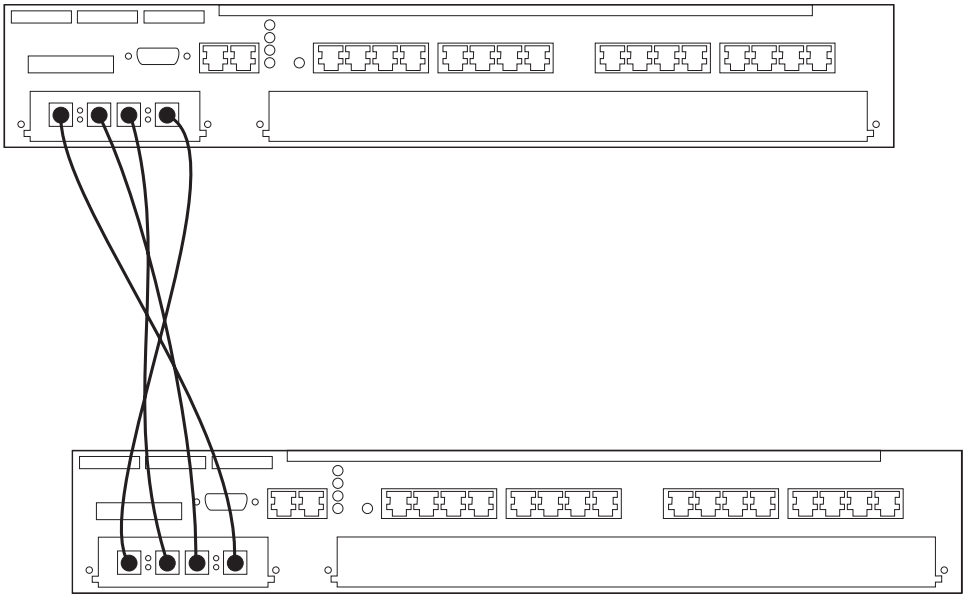

Figure 3-3. Cabling for the Optical Fiber RI/RO Module

     a. Connect the RI receive port to the RO transmit port on the external device.
     b. Connect the RI transmit port to the RO receive port on the external device.
     c. Connect the RO receive port to the RI transmit port on the external device.
     d. Connect the RO transmit port to the RI receive port on the external device.
   - For the RJ-45 RI/RO Module:

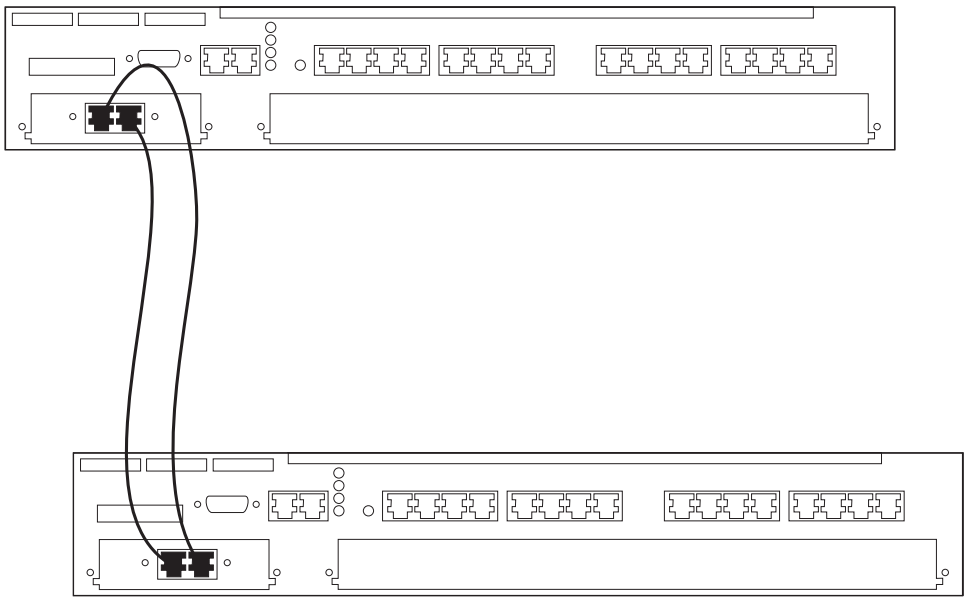

Figure 3-4. Cabling for the RJ-45 RI/RO Module

a. Connect RI on the 8239 to RO on the external device.

b. Connect RO on the 8239 to RI on the external device.

Attention:

- Be sure that you connect RI/RO cables at both ends before enabling these interfaces. Any of these interfaces that are not going to be used should be administratively disabled.
- Use caution when implementing a network with more than one RI/RO interface per stack. Multiple RI/RO connectors between two ring segments or between two 8239 Model 1s in the same stack can cause undesirable results, such as a division of the ring into two independent segments.

6. Provide power to the 8239.

   The RI/RO ports are disabled by default. To enable them, issue the ENABLE RING_IO command or the UNWRAP RING_IO command; these commands are equivalent.

Chapter 4. Configuration

This chapter describes the configuration procedures you need to perform before you can manage the 8239.

When you install an 8239, it contains factory-default parameters. Depending on your needs, you might want to change these defaults. For a listing of the default values, go to “Configuration Parameters” on page 4-9.

Using the Command Interface

Employ the command interface using a terminal emulation program that supports VT100 emulation or using Telnet over an IP connection.

Login Access

To use the terminal interface, you must enter a login name and password. There are two access types associated with a login name:

- Admin, which allows you to issue all commands
- User, which allows you to issue a subset of the commands allowed under Admin access.

Configuration changes made with User access can be saved only under Admin access. The SAVE command is not allowed for User access.

The default login name is “admin” with no password. It is recommended that you change the 8239 login password to a more secure password.

Management Using Emulation Software

You can use terminal emulation software in one of two ways:

- Using a direct, null-modem cable connection
- Using a public telephone network via a modem and a standard EIA-232 cable

The default terminal baud setting is 9600 bps. This value can be changed using the SET TERMINAL BAUD command. Initialization and diagnostic messages are displayed at 9600 bps; once the 8239 is operational, the configured terminal baud setting is used.

Using a Null-Modem Cable

To communicate with the 8239 for the first time, configure the terminal emulation application with:

- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control
- VT100 emulation
- The communications port of the workstation that is attached to the 8239

Using a Modem

If you will be communicating with the 8239 by means of a modem connection, you will need to install a second modem and connect it to your workstation.

Configure the terminal emulation application with:

- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control
- VT100 emulation
- The workstation's communication port that will be used

Establishing a Session

To establish a session:

1. Invoke emulation software to establish direct connection by means of the null-modem cable, or invoke the emulation software and dial the number of the modem attached to the 8239.
2. After the connection is established, you will see either:
   - The login prompt or trap messages (if the 8239 is already powered on)
   - Diagnostic messages (if you provide power after establishing the connection)
3. Press **Enter** two or three times.
4. At the login prompt, type **admin** and then press **Enter** (ADMIN is the default user name).
5. You are now logged on.

Management Using Telnet

You can access the 8239 in-band using Telnet to an 8239 Model 1. To configure the 8239 Model 1 for in-band connectivity, go to "Configuring the 8239 for In-Band Connectivity" on page 4-5.

Command Interface Conventions

The main panel of the command interface for an 8239 Model 1 is shown below.

```
8239 Login Prompt
Login:admin
Password:mypassword

Main Menu - Accepted inputs:
  1) bootp                              10) replicate
  2) clear                              11) reset_hub
  3) disable                            12) restore_to_factory_default
  4) display                            13) retrieve
  5) enable                             14) save
  6) help                               15) set
  7) load                               16) script
  8) logout                             17) unwrap
  9) ping                               18) wrap

  Type 'help' for information

?=Help>
```

Note: When the password is null (the default value), the line that prompts for password may not appear.

Once you have logged on to the 8239, manage the stack using the command interface. Use these guidelines, special keys, and short cuts:

- When a terminal interface command is issued, the command is displayed on the command line until execution of the command is completed. Be aware that traps may appear on the terminal while execution of a command is in process.
- Pressing **Esc** returns you to the terminal prompt.
- Pressing **shift** and **?** displays a list of the values that you can enter for a particular command.
- Default values or current settings are shown in brackets.
- Pressing **Enter** accepts the value shown in brackets.
- Commands are not case sensitive.
- Commands can be issued by:
  - Typing the entire command.
  - Typing part of the command and pressing the space bar.
  - Typing the number shown next to the command. The numbers representing a command are not the same on the 8239 Model 1 and the Model 2.
- Pressing **Tab** selects the first command that matches what you typed. Repeatedly pressing **Tab** cycles through the possible commands that match what you typed.
- Up to 10 previously entered commands that have completed execution can be recalled, edited, if necessary, and then executed. To retrieve commands, simultaneously press:
  - **Ctrl** and **R** to recall the last entered command
  - **Ctrl** and **F** to go forward in the command history
  - **Ctrl** and **B** to go backward in the command history

  To edit a recalled command, press **Backspace** until you reach what needs changing, type the new information, and press **Enter**.

  Note: Commands can be recalled only if the command has completed execution. For example, if you enter DISPLAY NETWORK_MAP ALL_STATIONS and press **Esc** before the last entry is display, then the DISPLAY NETWORK_MAP ALL_STATIONS command will not be in the recall list.
- Entering **help** at the terminal prompt displays hints about performing routine tasks.

Examples

The following table describes how to perform some common management tasks using the terminal interface. The examples assume this stack configuration:

- The stack consists of one 8239 Model 1 and two 8239 Model 2s.
- The 8239 Model 1's hub ID is 1; the hub IDs of the 8239 Model 2s are 2 and 3.
- Hub 1 contains the RI/RO Module.
- IP is to be configured on hub 1. The IP address is 9.197.4.67, the subnet mask is 255.255.255.0, and the default gateway is 9.197.4.1.

- The ASCII terminal is connected to the 8239 Model 1s (hub 1) EIA-232 port.

Task	Action
Remove an external device and its ports from the stack data ring	Type **wrap ring_io both 1** and press **Enter**.
Insert an external device and its ports into the stack data ring	Type **unwrap ring_io both 1** and press **Enter**.
Remove hub 2 from the stack data ring	Type **wrap data_io both 2** and press **Enter**.
Insert hub 2 into the stack data ring	Type **unwrap data_io both 2** and press **Enter**.
Set up IP on hub 1	Type **set ip 1** and press **Enter**. When prompted, enter the following information, pressing **Enter** after each value: IP address: Type **9.197.4.67** Subnet mask: Type **255.255.255.0** Default gateway: Type **9.197.4.1**
Get status for the stack	Type **display stack** and press **Enter**.
Get status for hub 2	Type **display hub 2** and press **Enter**.
Get status for port 4 on hub 2	Type **display port 2.4** and press **Enter**.
Enable all ports on hub 1	Type **enable port 1.all** and press **Enter**.
Disable port 4 on hub 2	Type **disable port 2.4** and press **Enter**.

Verifying, Saving, and Restoring Parameters

Verifying Parameters

To verify parameters that you have entered, type the appropriate DISPLAY command.

Saving Parameters

If you change configuration settings and then the 8239 Model 1 loses power or is reset before you save the changes, the changes are lost; the last-saved configuration settings are used. For this reason, you should save configuration information frequently.

To save the current configuration for all the 8239s in the stack, type **save** and press **Enter**.

Restoring Parameters

To restore the last-saved configuration for all hubs in the stack, reset the 8239 without saving the configuration.

Configuring the 8239

This section explains how to configure the 8239 for:

- Out-of-band connectivity
- In-band connectivity
- Network monitoring

See “Configuration Parameters” on page 4-9 for a list of configuration parameters.

Configuring the 8239 for Out-of-Band Connectivity

The 8239 supports out-of-band access on both models through the EIA-232 port. You can attach either an ASCII terminal for local access or a modem for remote access. The 8239 default settings support out-of-band connectivity. To change any configuration settings, use the SET TERMINAL command. See “Connecting an ASCII Terminal or Modem to the EIA-232 Port” on page 2-5 for instructions for connecting to the EIA-232 port. See “Using the Command Interface” on page 4-1 for information about the command interface.

Configuring the 8239 for In-Band Connectivity

In-band connectivity lets you access the 8239 Model 1 from a remote station using the Token-Ring network rather than an EIA-232 port. In order to use in-band connectivity, the 8239 Model 1 must be configured with IP information. You can configure IP information initially using either of these methods:

- BOOTP
- Terminal interface commands via the EIA-232 port

BOOTP

If you do not plan to use BOOTP, you should use the DISABLE BOOTP command in order to reduce network traffic. Continue with this section only if you are interested in in-band connectivity; otherwise, go to “Using the Command Interface” on page 4-1.

BOOTP (boot protocol) is a user datagram protocol/internet protocol (UDP/IP)-based protocol that allows a 8239 Model 1 to obtain IP information with the assistance of a BOOTP server; with the IP information, the 8239 can use in-band connectivity. The 8239 supports BOOTP to facilitate the configuration of newly installed stacks in remote locations. Every 8239 Model 1 is shipped with the BOOTP protocol enabled.

If your installation has only 8239 Model 2s, in-band connectivity is not supported.

Configuration Using BOOTP: A newly installed 8239 Model 1 broadcasts a BOOTP request over IP when it is powered on or reset. The BOOTP server, using information from its BOOTPTAB file, provides the 8239 Model 1 with configuration information. In addition to obtaining the IP address and the subnet mask, the 8239 Model 1 can attach to a configuration server to obtain a configuration file. The configuration file is an ASCII file containing 8239 commands. The commands are executed as soon as the configuration file is transferred via TFTP to the 8239. The 8239 Model 1 updates its configuration with the information contained in the BOOTP message. The following example of a BOOTPTAB file entry contains configuration information for the 8239:

ibm8239hub1:*ha*=0006298f0490:*ip*=200.0.0.163:*sm*=255.255.255.0
:*gw*=200.0.0.150:*sa*=200.0.0.150:*bf*=/tmp/hub1.pfl:*ht*=6

where

ha	Is the hardware address of the 8239
ip	Is the IP address of the 8239
sm	Is the subnet mask of the 8239
gw	Is the default gateway
sa	Is the server IP address from which the configuration file is transferred via TFTP
bf	Is the configuration file name
ht	Is the hardware type (“6” specifies Token Ring)

Configuration information obtained from the BOOTP server is not saved unless you issue a SAVE command.

If your network administrator is using BOOTP to configure network devices, contact the administrator to determine if you need to make any configuration changes.

Terminal Interface Commands Through the EIA-232 Port

To remotely manage the 8239 or remotely monitor the network using the EIA-232 port, set the IP addresses of the Management Interface hub:

- **set ip** *hub_id ip_address subnet_mask default_gateway*

Management Interface Insertion

Make sure that the Management Interface is inserted into the ring:

set management_interface administrative_mode enable *hub_id*

SNMP Access

1. Set the community table information, if appropriate, using the SET COMMUNITY command. Telnet does not require this information.
2. Set the access control list information, if appropriate, using SET ACCESS ACCESS_CONTROL_LIST

   Note: Because the initial state grants wide access to well-known communities, it is recommended that you change the 8239 default configuration to a more secure configuration.
3. Set the trap community information, if appropriate, using SET TRAP_COMMUNITY.

Changing Token-Ring Options

By default, the 8239 Model 1 is configured as a station on the Token-Ring network using the ring speed that was configured for the hub and the default MAC address. However, if you want, you can:

- Specify a locally administered MAC address

  The 8239 Model 1 is produced with a factory-set MAC address. If you want to use a locally administered MAC address, follow these steps.

  1. Specify the MAC address:

set management_interface locally_administered_address *hub_id mac_address_value*

2. Specify the use of the locally administered MAC address:

   set management_interface mac_address_type locally_administered *hub_id*

Changing the MAC address type to locally administered causes the Management Interface to close and reopen its adapter.

- Set other Token-Ring options.

  To set other Token-Ring network options, issue the appropriate SET MANAGEMENT_INTERFACE command.

Configuring for Network Monitoring

To configure the 8239 for network monitoring, enter these commands.

1. If you are going to use in-band management, configure the 8239 according to the instructions in “Configuring the 8239 for In-Band Connectivity” on page 4-5.
2. Enable the data-gathering functions that you need:
   - To enable the 8239 for RMON, go to “Configuring RMON.”
   - To configure the 8239 as a surrogate function, go to “Configuring for the Surrogate Agent” on page 4-8.

Configuring RMON

To configure RMON:

- Assign IP information if you are accessing RMON information via in-band connectivity. The RMON manager must have a physical path to the 8239’s RMON probe.
- For security reasons, you may want to change the default community names and set up access control lists
- If source routing is used on the segment and an RPS is not on the ring, you must set the ring segment number in order for the RMON source routing statistics to be accurate. For information about setting the ring segment number, see “Enabling RPS” on page 4-8.

By default, all RMON groups are enabled and some RMON groups are set up automatically. You can disable individual RMON groups using a terminal interface command or via SNMP through the 8239 private MIB. For more information, go to Chapter 7, 8239 Device Management.

Example: To configure the 8239 to communicate with an Nways Campus Manager — Remote Monitor (ReMon), follow these steps.

1. Make sure that the 8239 Model 1 that is acting as an RMON probe is configured with the appropriate IP information by using the DISPLAY IP ADDRESS command. If a change is necessary, configure the IP information using the following command:

   set ip *hub_id ip_address subnet_mask default_gateway*

2. Follow the instructions provided with ReMon to configure or add a device or probe.

Configuring for the Surrogate Agent

Enabling the Token-Ring surrogate function involves enabling the surrogate group and, possibly, the CRS, REM, and RPS groups.

Note that almost all information associated with the surrogate agent can also be accessed via SNMP through the IBM TR Surrogate MIB. Accessible only through the 8239 MIB are:

- surrogate group administrative mode
- rps_traps administrative mode

Enabling the Surrogate Group: Use one of these methods:

- Issue this command:

  set management_interface surrogate_group enable

- Issue this command:

  enable tr_surrogate surr_status surr_admin

- Use SNMP through the IBM 8239 TR Hub MIB.

Enabling REM

1. Enable the surrogate group as explained in “Enabling the Surrogate Group.”
2. Enable the REM function using this command:

   enable tr_surrogate surr_status rem_admin

3. Enable each REM flag that you need using this command:

   enable tr_surrogate rem_status *option*

   Note: rem_traps defaults to enabled; all other flags default to disabled.

Enabling CRS

1. Enable the surrogate group as explained in “Enabling the Surrogate Group.”
2. Use this command to enable the CRS function:

   enable tr_surrogate surr_admin crs_admin

3. Enable the CRS to report topology change traps:

   enable tr_surrogate crs_traps

   The default value for crs_traps is enabled.

Enabling RPS

1. Enable the surrogate group as explained in “Enabling the Surrogate Group.”
2. Enable RPS using this command:

   enable tr_surrogate surr_admin rps_admin

3. Use this command to enable RPS to report new stations inserted into the ring:

   enable tr_surrogate rps_traps

   The default value for rps_traps is enabled.

RPS does not become active until you set the ring segment number. A ring segment number is the part of the virtual storage ring address needed to refer to a

segment. It is used for identification of Token-Ring segments that are being remotely monitored. Set the ring segment number if the 8239 Model 1 is acting as the Ring Parameter Server, or if there is no Ring Parameter Server on the segment and you are collecting RMON source routing statistics. Use the Token-Ring Surrogate function to identify or set a ring segment number.

The ring segment number can also be obtained with the Aspen Config MIB.

To set the ring segment number, use one of these methods:

- Enter the following command:

  set tr_surrogate segment_number *segment_number*

- Use an application that supports SNMP or use a MIB browser to set the value in the Token_Ring Surrogate MIB.

Configuration Parameters

The following table lists all 8239 parameters, their defaults, and whether they are configurable. An asterisk following a parameter means that the parameter is configurable from both an 8239 Model 1 and Model 2; otherwise, a parameter is configurable from a Model 1 only.

Parameters that are not configurable provide status and information. If a parameter is configurable and the default value is “N/A”, there is no default value and the parameter must be set. If a parameter is not configurable and the default is “N/A”, the parameter is read only; the value is provided by the product.

These parameters are accessible using the command interface or using SNMP through the 8239 MIB.

Parameter	Default Value	Configurable
Access Control list (level 4)	Any IP address with level 4 community name	Yes
Access Control list (level 3)	Any IP address with level 3 community name	Yes
Access Control list (level 2)	Any IP address with level 2 community name	Yes
Access Control list (level 1)	Any IP address with level 1 community name	Yes
Beacon threshold*	8	Yes
BOOTP power-up mode	ENABLED	Yes
BOOTP server IP address	255.255.255.255	Yes
Clock	Initially, JAN 21 00:00:00 1997	Yes
Community name (level 1)	PUBLIC	Yes
Community name (level 2)	RMON	Yes
Community name (level 3)	USER	Yes
Community name (level 4)	ADMIN	Yes
Control In administrative mode*	UNWRAPPED	Yes
Control Out administrative mode*	UNWRAPPED	Yes

Parameter	Default Value	Configurable
Data In administrative mode*	UNWRAPPED	Yes
Data Out administrative mode*	UNWRAPPED	Yes
Dot5 group	DISABLED	Yes
Event script	N/A	Yes
Group mode*	N/A	Yes
Group name*	N/A	Yes
Group port*	N/A	Yes
Hub ID*	Lowest available value	Yes
IP address	0.0.0.0	Yes
IP default gateway	0.0.0.0	Yes
IP subnetwork mask	0.0.0.0	Yes
Login user*	ADMIN with no password	ID and password can be configured
Management Interface active monitor participation	DISABLED	Yes
Management Interface Adapter microcode version	READ-ONLY	No
Management Interface Adapter status	READ-ONLY	No
Management Interface administrative mode	ENABLED	Yes
Management Interface ARP resolve method	SOURCE-ROUTE	Yes
Management Interface burned-in MAC address	xx-xx-xx-xx-xx-xx	No
Management Interface diag wrap	None	Yes
Management Interface early token release	ENABLED	Yes
Management Interface locally administered address	00-00-00-00-00-00	Yes
Management Interface MAC address type	BURNED-IN	Yes
Operational version*	Initially, v1.0	No
Port speed detect*	ENABLED	Yes
Port trap*	ENABLED	Yes
Port 8228 mode*	DISABLED	Yes
Port administrative mode*	ENABLED	Yes
Ports main administrative mode (ports 1-16)*	UNWRAPPED	Yes
Ports expansion administrative mode (feature slot)*	UNWRAPPED	Yes
Purge on insert*	ENABLED	Yes
Surrogate REM trap flag	ENABLED	Yes
REM individual flag settings	DISABLED	Yes
Ring In administrative mode	DISABLED	Yes
Ring Out administrative mode	DISABLED	Yes
Ring segment number	Value from RPS, last saved value, or 0	Yes

Parameter	Default Value	Configurable
Ring speed*	16Mbps	Yes
RMON Alarm group	ENABLED	Yes
RMON Event group	ENABLED	Yes
RMON History_ML group	ENABLED	Yes
RMON History_P group	ENABLED	Yes
RMON Host group	ENABLED	Yes
RMON Matrix group	ENABLED	Yes
RMON RingStation group	ENABLED	Yes
RMON Statistics Mac_Layer group	ENABLED	Yes
RMON Statistics Promiscuous group	ENABLED	Yes
RMON Statistics Sourcerouting group	ENABLED	Yes
RMON TopN group	ENABLED	Yes
RMON2 Mode	RMON2	Yes
Security action on intrusion*	TRAP-ONLY	Yes
Security mac_address*	N/A	Yes
Security mode*	DISABLED	Yes
Serial port baud rate*	9600	Yes
Serial port data bits*	8	No
Serial port parity*	NONE	No
Speed mismatch threshold*	8	Yes
Surrogate CRS Admin status	DISABLED	Yes
Surrogate CRS trap flag	ENABLED	Yes
Surrogate group	DISABLED	Yes
Surrogate REM Admin status	DISABLED	Yes
Surrogate REM trap flag	ENABLED	Yes
Surrogate RPS Admin status	DISABLED	Yes
Surrogate RPS trap flag	ENABLED	Yes
System contact	N/A	Yes
System description	8239, SW_version, hub_id	No
System location	N/A	Yes
System name	8239	Yes
Terminal prompt*	?=Help>	Yes
Terminal timeout	No time-out for EIA-232 port; 15 min. for Telnet	No
TFTP file name	N/A	Yes
TFTP server IP address	N/A	Yes
Trap authentication	ENABLED	Yes
Trap community	N/A	Yes
Trap console display*	ENABLED	Yes
Trap control IO status up/down*	ENABLED	Yes

Parameter	Default Value	Configurable
Trap data IO status up/down*	ENABLED	Yes
Trap multiple users	ENABLED	Yes
Trap port security intrusion*	ENABLED	Yes
Trap port up/down*	ENABLED	Yes
Trap ring IO status up/down	ENABLED	Yes
Trap RMON	DISABLED	Yes
Trap script	ENABLED	Yes

Chapter 5. Problem Determination Procedures

When problems occur, use these diagnostic tools:

- The front panel LEDs (“Using the LEDs to Diagnose Problems”)
- The LCD messages (“LCD Messages” on page 5-15) on the 8239 Model 1 serving as your management unit
- The Symptom Chart (“Summary of Symptoms and Problem Determination Procedures” on page 5-17)

Before performing problem determination or contacting your provider of service because you are unable to solve a problem, it is suggested that you obtain the information listed in “General Information about the 8239” on page 5-24.

For additional information about problem determination, refer to the *Token-Ring Problem Determination Guide*, (SX27-3710).

Using the LEDs to Diagnose Problems

All 8239s have LEDs that indicate the status of some of their components. The following types of LEDs are provided on the front panel of an 8239:

- Power indicator
- Box status (OK LEDs)
- Ring speed indicator
- Port status
- RI/RO status (Model 1 only)
- Stack In/Stack Out status

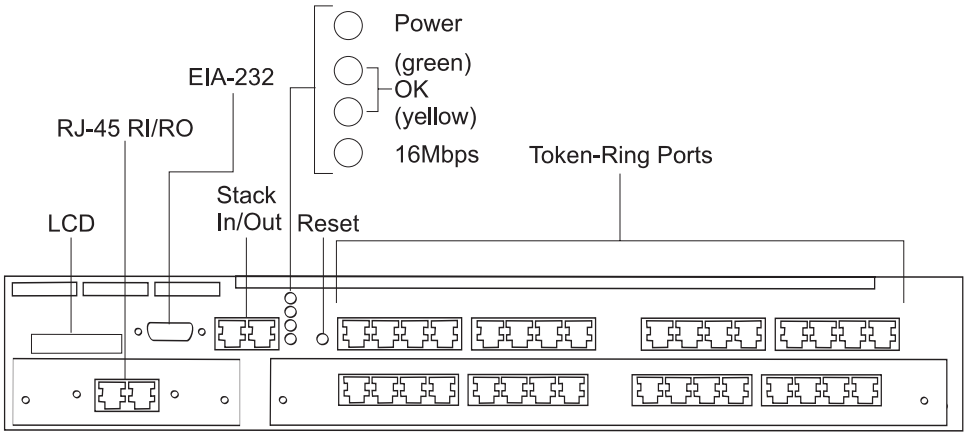

Figure 5-1. 8239 Model 1 LEDs and LCD

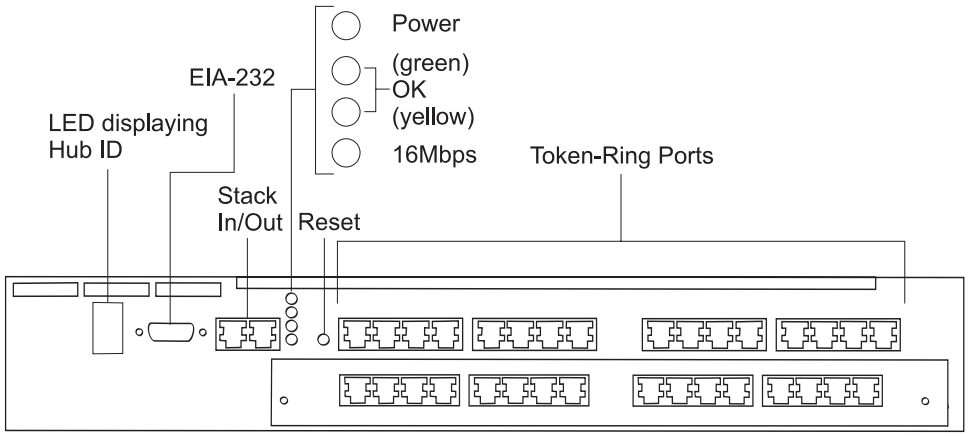

Figure 5-2. 8239 Model 2 LEDs

Power Indicator

Table 5-1. Power Indicator (Green LED)

State	Meaning	
On	8239 is receiving power.	
Off	Unit has no power or there is a failure	
	Cause	**Action**
	8239 power cord is disconnected	Connect the power cord.
	8239 power cable is defective	Replace the power cord.
	Power outlet is not supplying power	Check the power outlet.
	Power supply failure	If the fans are not running, replace the power supply.
	8239 failure	Replace the 8239.
	LED failure	If other LEDs work, the LED has failed. Replace the 8239.

Box Status

Table 5-2. Box Status (OK LEDs)		
Green	**Yellow**	**Meaning**
On	Off	Unit is operational
Off	On	During POST, DRAM test is running
Blinking	Blinking	Boot code or POST is running. If the blinking lasts for more than 2 minutes, unit not operational; for the cause of this hardware failure, go to “LCD and LED Codes” on page 5-14.
On	On	If this LED state lasts for less than 30 seconds, the operating system is initializing during bringup. If this state lasts for 30 seconds or more, the unit is not operational. For the cause of this hardware failure, go to “LCD and LED Codes” on page 5-14.
On	Blinking	Unit is executing beacon recovery.
Off	Off	If indicators remain off for more than 2 minutes, unit is not operational.

Ring Speed

Table 5-3. Ring Speed (Green LED)	
State	**Meaning**
On	16-Mbps ring speed
Off	4-Mbps ring speed

Port Status

One green and one yellow LED is associated with each port; they are located above each port.

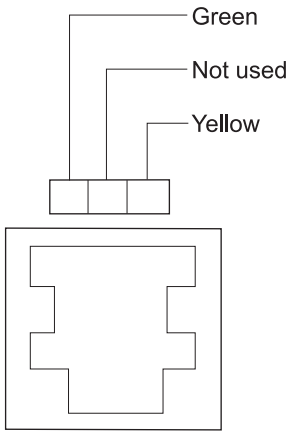

Figure 5-3. Port Status LEDs

These status descriptions are valid only when:

- The power indicator LED is on
- The box status green LED is on
- Box status yellow LED is not on

Port Status Green LED

Table 5-4. Port Status (Green LED)

State	Meaning
On	Port is inserted and operational. Exception: if both the green and yellow box status LEDs are on, the port has failed diagnostics.
Off	Port is not inserted If the yellow port LED is on or blinking, go to “Port Status Yellow LED.” **Cause** — **Action** No station is connected — If required, connect station. The connected station is powered off or the workstation is not operating — Make sure the station is powered on and the workstation is operating correctly. Cabling problem — Make sure that all cable connections are secure. Check the cable for breaks or other damage. Replace suspect cables with cables that are known to be good. Make sure the cable length and specifications comply with the requirements in “Cable Types and Distances” on page 1-4. Station speed mismatch — Make sure that the ring speed of the connected station matches the hub ring speed.
Blinking	Port is administratively disabled **Cause** — **Action** User disabled the port — If required, use ENABLE PORT to enable the port. See *Command Reference* for information about this command.

Port Status Yellow LED

Table 5-5. Port Status (Yellow LED)

State	Meaning
On	Port is wrapped due to wrong speed or beacon error. Use DISPLAY PORT to obtain the port status. **Cause** — **Action** Cabling problem when port status is BEACON WRAPPED — Make sure that all cable connections are secure. Check the cable for breaks or other damage. Replace suspect cables with cables that are known to be good. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Workstation failure when port status is BEACON WRAPPED — Make sure the workstation is installed and operating correctly. Workstation entered at the wrong speed when port status is SPEED MISMATCH — Make sure the workstation is configured for the same ring speed as the 8239. Ring speed can be 4 or 16 Mbps. Ring speed LEDs on the front panel indicate the ring speed. Use DISPLAY PORT for more information.
Off	Port does not have a fault.
Blinking	The port is administratively disabled due to security violation or threshold exceeded. Use DISPLAY PORT to obtain the port status. **Cause** — **Action** A MAC address that is not in the port's security table was inserted at that port when port status was SECURITY BREACH — If it is OK for that workstation to be inserted at that port, add the workstation's MAC address to the port's security table (using SET SECURITY_PORT MAC_ADDRESS) or disable port security (using DISABLE SECURITY_PORT). A workstation has exceeded threshold for entering at the wrong speed when port status is SPD THRES ERROR — Make sure the workstation is configured for the same ring speed as the 8239. Ring speed can be 4 or 16 Mbps. Ring speed LEDs on the front panel indicate the ring speed. Use DISPLAY PORT for more information. The port has exceeded the threshold for beacon faults when port status is BCN THRES ERROR — Beaconing is typically due to a faulty workstation NIC or lobe cable. Use DISPLAY PORT for more information. Resolve the fault.

A port that is administratively disabled remains in that state until the command is issued to enable or disable the port. The administratively disabled state takes precedence over any other state. For example, if a port is administratively disabled due to a beacon threshold being exceeded and the cable is removed from the port,

the port will still be administratively disabled. Once a port has been administratively disabled, issue the ENABLE PORT command to allow insertion of the port again.

RI/RO Status

One green and one yellow LED are associated with each port.

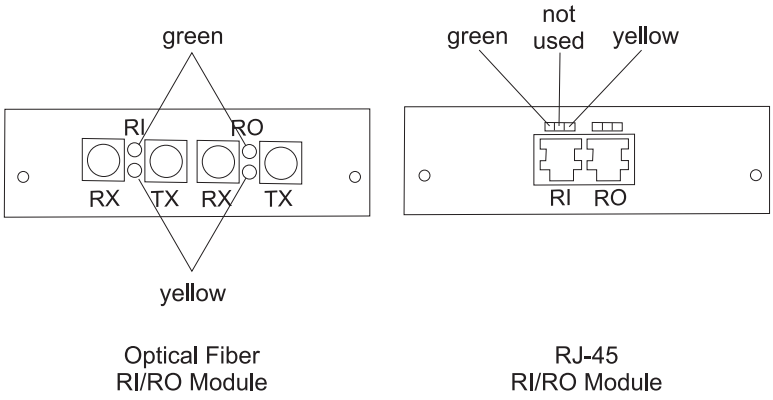

Figure 5-4. RI/RO LEDs

Note: These status descriptions are valid only when:

- The power indicator LED is on
- The box status green LED is on
- Box status yellow LED is not on

Note: When the 8239 is reset, all of the RI/RO LEDs are on during the DRAM test. In addition, the box status green LED is off and the yellow LED is on.

RI/RO Status Green LED

Table 5-6. RI/RO Status (Green LED)

State	Meaning	
On	RI/RO is inserted	
Off	RI/RO is not inserted	
	Cause	**Action**
	Cabling problem	Make sure all cable connections are secure. Go to “RI/RO Module” on page 3-2; check the cabling. Check the cabling for breaks or other damage. Replace suspect cables with known good cables. If you are using the Optical Fiber RI/RO Module, note that bending the fiber beyond the minimum bend radius can break the internal fiber while the cable jacket remains undamaged. Make sure the cable length and specifications comply with the requirements in “Cable Types and Distances” on page 1-4.
	Remote device not powered on	Power on the remote device.
Blinking	RI/RO is administratively disabled	

RI/RO Status Yellow LED

Table 5-7. RI/RO Status (Yellow LED)

State	Meaning	
On	RI/RO is wrapped due to beaconing	
	Cause	**Action**
	Cabling problem	Make sure all cable connections are secure. Go to "RI/RO Module" on page 3-2; check the cabling. Check the cabling for breaks or other damage. Replace suspect cables with known good cables. If you are using the Optical Fiber RI/RO Module, note that bending the fiber beyond the minimum bend radius can break the internal fiber while the cable jacket remains undamaged. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4.
	Fault is on the remote device	Resolve the problem at or off of the remote device. The 8239 will automatically unwrap the RI/RO connector that was wrapped once it detects that the connection is good. You may also use ENABLE RING_IO to unwrap the RI/RO connector.
Off	RI/RO is OK	

Stack In/Stack Out Status

Three LEDs are associated with each Stack-In and Stack-Out connection. The LEDs for each connection are physically located over that connection. The LEDs provide information about the data path and the control path that make up a stack connection. The Stack-In connection is made up of Data In and Control In; the Stack-Out connection is made up of Data Out and Control Out.

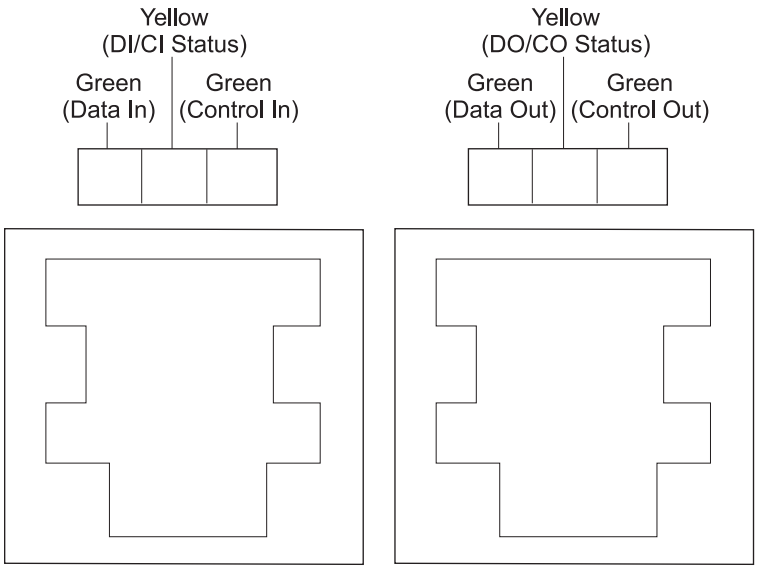

Figure 5-5. Stack In/Stack Out LEDs

Table 5-8 and Table 5-9 on page 5-11 describe LED states for Stack In and for Stack Out.

Note: These status descriptions are valid only when:

- The power indicator LED is on
- The box status green LED is on
- Box status yellow LED is not on

Stack-In Status

Table 5-8 (Page 1 of 4). Stack-In Status

Green (Data In)	Yellow (DI/CI Status)	Green (Control In)	Meaning
On	Off	On	Normal: Data In is unwrapped; Control In is unwrapped.
Blinking	Off	On	No faults detected; Data In has been wrapped by system administrator. **Action:** If required, use UNWRAP DATA_IO.
On	Off	Blinking	No faults detected. Control In has been wrapped by system administrator. **Action:** If required, use UNWRAP CONTROL_IO.
Blinking	Off	Blinking	No faults detected. Data In and Control In have both been wrapped by the system administrator. **Action:** If required, use UNWRAP DATA_IO and UNWRAP CONTROL_IO.

Table 5-8 (Page 2 of 4). Stack-In Status

Green (Data In)	Yellow (DI/CI Status)	Green (Control In)	Meaning
Off	On	On	Fault detected in Data In; Data In is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cabling problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.
Off	On	Off	Fault detected in both Data In and Control In; both are wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

Table 5-8 (Page 3 of 4). Stack-In Status

Green (Data In)	Yellow (DI/CI Status)	Green (Control In)	Meaning
Off	On	Blinking	Fault detected in Data In and Data In is wrapped. No fault on Control In but Control In has been wrapped by the system administrator. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in “Cable Types and Distances” on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.
On	On	Off	Fault detected in Control In; Control In is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in “Cable Types and Distances” on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

Table 5-8 (Page 4 of 4). Stack-In Status

Green (Data In)	Yellow (DI/CI Status)	Green (Control In)	Meaning
Blinking	On	Off	No fault on Data In, but Data In has been wrapped by system administrator. Fault detected in Control In and Control In is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

Stack-Out Status

Table 5-9 (Page 1 of 4). Stack-Out Status

Green (Data Out)	Yellow (DO/CO Status)	Green (Control Out)	Meaning
On	Off	On	Normal: Data Out is unwrapped; Control Out is unwrapped.
Blinking	Off	On	No faults detected; Data Out has been wrapped by system administrator. **Action:** If required, use UNWRAP DATA_IO.
On	Off	Blinking	No faults detected. Control Out has been wrapped by system administrator. **Action:** If required, use UNWRAP CONTROL_IO.
Blinking	Off	Blinking	No faults detected. Data Out and Control Out have both been wrapped by the system administrator. **Action:** If required, use UNWRAP DATA_IO and UNWRAP CONTROL_IO.

Table 5-9 (Page 2 of 4). Stack-Out Status

Green (Data Out)	Yellow (DO/CO Status)	Green (Control Out)	Meaning
Off	On	On	Fault detected in Data Out; Data Out is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack Out connects to Stack In. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.
Off	On	Off	Fault detected in both Data Out and Control Out; both are wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack Out connects to Stack In. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

Table 5-9 (Page 3 of 4). Stack-Out Status

Green (Data Out)	Yellow (DO/CO Status)	Green (Control Out)	Meaning
Off	On	Blinking	Fault detected in Data Out and Data Out is wrapped. No fault on Control Out but Control Out has been wrapped by the system administrator. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.
On	On	Off	Fault detected in Control Out; Control Out is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack Out connects to Stack In. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

Table 5-9 (Page 4 of 4). Stack-Out Status

Green (Data Out)	Yellow (DO/CO Status)	Green (Control Out)	Meaning
Blinking	On	Off	No fault on Data Out but Data Out has been wrapped by system administrator. Fault detected in Control Out and Control Out is wrapped. **Cause** — **Action** Stack cable connected to incorrect port — Make sure that Stack In connects to Stack Out. Cable problem — Make sure all cable connections are secure. Check the cable for breaks or other damage. Make sure the cable length and specifications comply with the requirements in "Cable Types and Distances" on page 1-4. Replace suspect cables with known good cables. Allow one minute after each replacement for problem to clear. Hardware failure — Isolate the faulty 8239 and replace it.

LCD and LED Codes

The Model 1 LCD and the Model 2 LED display two types of messages:

- POST codes
- Operational codes

POST Codes

POST codes are the same on both the Model 1 LCD and the Model 2 LED display. At the beginning of POST, the green and yellow box status LEDs start blinking simultaneously. They blink until POST is completed.

Table 5-10 on page 5-15 shows the letters displayed at each stage of POST and the action that should be taken if the POST stops at that stage and displays one of the letters.

Table 5-10. POST Codes	
Display	**Action**
A, B, C, D, E, F, G, H, no display	1. Press the Reset button. If the problem remains, continue with step 2 on page 5-15. 2. Remove any optional features (see Chapter 3, “Installing Features” on page 3-1 for instructions) and press the Reset button again. 3. If the problem remains, replace the base unit. 4. Install features into new base unit, using the instructions in Chapter 3, “Installing Features” on page 3-1.
I, J	Replace the RI/RO Module, using the instructions in Chapter 3, “Installing Features” on page 3-1. If the problem remains, replace the base unit.
M	Replace the 16-Port Expansion Adapter, using the instructions in Chapter 3, “Installing Features” on page 3-1. If the problem remains, replace the base unit.
N, O	1. Press the Reset button. If the problem remains, continue with step 2 on page 5-15. 2. Remove any optional features 3. Replace the base unit 4. Install features into new base unit

Any failure is considered irrecoverable. A failure prevents further system initialization. Error codes are displayed. The 8239 stops with the green and yellow box status LEDs on.

After a successful POST, the LCD indicates that the diagnostic tests are complete by displaying the hub ID.

Operational Codes

LED Display Message

The 8239 Model 2 has a single-segment LED. During POST, the LED indicates the progress of the diagnostic tests by displaying letters representing each test; the same letter with a detailed test name and status is shown on the terminal interface during the diagnostic tests. After POST is completed and the hub ID is assigned, the hub ID is displayed.

LCD Messages

The LCD on the 8239 Model 1 is a 2 x 16-character display.

During bring-up, any messages that appear on the LCD when the LCD light is off are not valid.

During POST, the LCD indicates the progress of the diagnostic tests by showing letters representing each test; the same letter with a detailed test name and status is shown on the terminal interface during diagnostic tests. After POST is finished, the LCD shows the operational code version for about 5 seconds; this message has the format:

OpCode *Release.Version*

During normal operation, the LCD shows:

- The hub ID for the Model 1
- Management Interface status
- Abbreviated text for selected traps

Trap text consists of a numeric value followed by a few descriptive words. All possible trap messages are documented in “Operational Codes” on page 5-15.

The format of the LCD when the 8239 Model 1 is operational is:

hub_id >unit type value trap_info
management_interface_status **>** *more_trap_info*

The LCD is updated every two seconds. A message remains on the LCD until another condition causes a different message to be displayed. Some messages (for example, traps and adapter status changes) may not be seen if multiple messages occur before the LCD is updated.

A description of each line on the LCD when the Model 1 is operational follows.

Line 1: *hub_id* **>***unit type value trap_info*

where

hub_id is a three-character field consisting of two blank spaces followed by a one-character hub ID of this stack unit.

unit has a value of 0 if the trap is being reported for a device external to the stack or is equal to the hub ID if the trap is being reported for a specific hub.

type has a value of “E” (error) or “I” (informational).

value is a 2-digit number identifying the specific trap.

trap_info further describes the trap using up to seven characters.

Line 2 : *management_interface_status* **>** *more_trap_info*

where

management_interface_status

is a 3-character code giving the management-interface adapter status or the ring number. The management-interface adapter status reflects the state of the token-ring interface used for 8239 in-band connectivity. These status codes are:

ber Management Interface exceeded the hub’s beacon threshold error value.

bwr Management Interface is beacon-wrapped.

cls Management Interface is closed.

dwr Management Interface is in diagnostic wrap mode.

opn Management Interface is open and unwrapped; Management Interface is inserted in the ring.

rst Management Interface is in the reset state.

wrp Management Interface administrative_mode is disabled; Management Interface is wrapped. This status code takes precedence over bwr, cls, and opn.

If the Management Interface is unwrapped and open, and a ring number is known for the ring, the display shows a 3-digit hexadecimal number representing the ring number, rather than a status of opn.

more_trap_info contains up to 11 characters further describing the message

For example, the message:

```
  1>2E03 Version
142>Mismatch
```

means that hub 1 is reporting on its display that hub 2 has an error and that the error is associated with message 3. The error is that the operational code version on hub 2 does not match hub 1. The message also indicates that the Management Interface is inserted in the network that has a ring segment number of 142.

Trap Message Number	Type	Text	Meaning
01	I	Hub Up	8239 is operational
02	E	Hub Down	8239 is not operational
03	E	Version Mismatch	Code version mismatch
04	I	RI/RO *wrap status* (see note)	RI/RO wrap status
05	I	DI/DO *wrap status* (see note)	Date In/Data Out wrap status
06	I	CI/CO *wrap status* (see note)	Control In/Control Out wrap status

Note: The wrap status is indicated with the terms “WRP” and “UNWRP”. For example, if Ring In is wrapped and Ring Out is unwrapped, the message text reads:

```
RI/RO WRP/UNWRP
```

Summary of Symptoms and Problem Determination Procedures

The following chart identifies various symptoms that can be seen with your network or hub. The referenced procedure describes the symptoms in more detail and provides problem determination procedures.

Symptom	Go To Page
Unable to communicate with the Management Interface	5-18
User station unable to insert into the network	5-19
User station having connectivity problems	5-20
8239 LEDs indicate an error condition	5-20
Beaconing on the data network	5-21
Soft errors on the data ring	5-21
Hub resets unexpectedly	5-21
Unable to obtain information from other hubs in the stack	5-22
Unexpected Hub Down trap	5-22
Code Version Mismatch trap	5-22
Station is not listed in the network_map	5-23
Expected entry is not reported by RMON	5-23
Expected data not displayed on Nways Campus Manager Remote Monitor	5-24
CRS data not available	5-24

Symptoms

Unable to Communicate with the Management Interface

This section applies to the 8239 Model 1 only.

The Management Interface is used for in-band connectivity to the 8239 stack as well as for monitoring the network. Indications that you are unable to communicate with the Management Interface are:

- The 8239 Model 1 does not respond to a ping or a ping from the Model 1 does not complete successfully
- A Telnet session cannot be established to the 8239
- An SNMP application, such as Nways Campus Manager, indicates that there is a problem accessing the 8239

These symptoms can be caused by:

- Network configuration problems
- 8239 configuration problems
- Problems within the network
- Problems within the 8239

To identify and resolve the problem:

1. Verify that the 8239 is configured properly for in-band connectivity. See “Verify Management Interface Configuration for Connectivity” on page 5-25.
2. Verify that the 8239 Management Interface is inserted into the network. See “Verify that the Management Interface is Inserted” on page 5-25.
3. Verify that there is a physical path between the 8239 Model 1 and the station being used to communicate with the Model 1. See “Verify that a Physical Path Exists Between Two End Stations” on page 5-30.

4. Verify that a network problem is not preventing communications:
    a. See “Check for Hard Errors (Beaconing) on the Data Network” on page 5-31.
    b. See “Check for Soft Errors on the Data Network” on page 5-34.
5. Verify that the Management Interface is able to receive data. See “Check the Management Interface’s Receive Capability” on page 5-28.
6. Verify that the Management Interface is able to transmit data. See “Check the Management Interface’s Transmit Capability” on page 5-30.

If you are still unable to communicate with the 8239, then perform these steps:

- If the 8239’s Management Interface MAC address or IP address recently changed, the ARP cache in any devices in the path between the 8239 and the end station may need to be cleared. To clear the ARP cache, issue the CLEAR ARP_CACHE terminal interface command.
- From the station, issue a trace route request to the 8239 Model 1’s IP address. If the packet does not reach the segment on which the 8239 resides, there may be a problem with the network. Verify that both endpoints are operational and that there are no network problems.

User Station Unable to Insert into the Network

Stations may not insert successfully into the network due to problems:

- With port configuration
- With 8239 configuration
- Within the network
- Within the 8239
- Within the station or in the cables connecting the station to the hub

To identify and resolve the problem:

1. Determine if there is anything wrong with the port or station based on the port status when the port is trying to insert. See “Check Port Status” on page 5-39.
2. Determine if the station cannot complete the adapter insertion process due to receiver congestion. See “Check Station Receiver Congestion on Insert” on page 5-42.
3. Disable the port (using the DISABLE PORT terminal interface command) and then try to insert the station. To determine if the station was able to insert, issue DISPLAY PORT and look at the “Status” value for the appropriate port.
    a. If the station is able to insert successfully, the port’s status will be “Inserted”. To verify that a network problem is not preventing the station from inserting:
        1) See “Check for Hard Errors (Beaconing) on the Data Network” on page 5-31.
        2) See “Check for Soft Errors on the Data Network” on page 5-34.
        3) See “Check the Neighbor Notification Process” on page 5-45.
    b. If the station is not able to insert successfully, the port’s status will not be “PHANTOM”. There may be a problem with the station or the cables connecting the station to the hub.

Remember to re-enable the port using the ENABLE PORT terminal interface command.

User Station is having Connectivity Problems

A station attached to the 8239 may not be able to communicate with another station due to problems:

- With network configuration
- With station configuration
- Within either station
- Within the network
- Within the 8239

To identify and resolve the problem:

1. Verify that the port that the 8239 station is attached to is inserted into the network using the information in “Check Port Status” on page 5-39.
2. Verify that there is a physical path between the 8239 station and the station communicating with the 8239 station. See “Verify that a Physical Path Exists Between Two End Stations” on page 5-30.
3. Verify that a network problem is not preventing communication
   a. “Check for Hard Errors (Beaconing) on the Data Network” on page 5-31.
   b. “Check for Soft Errors on the Data Network” on page 5-34.
4. Verify that the 8239 station is able to receive data. See “Check the Receive Capability of the Station” on page 5-43.

If the station connected to the 8239 is still unable to communicate with another station, there may be a problem with the station or the application being used on the station. Some applications do not recover automatically after connectivity with another application is lost and the data path connection is restored, for example, after a hub reset. The station may need to be rebooted.

8239 LEDs Indicate an Error Condition

The LEDs on the front panel of the 8239 provide status information. A yellow LED that is on or blinking usually indicates an error condition. A green LED blinking can sometimes indicate an error condition. For a complete description of all of the 8239 LEDs, refer to “Using the LEDs to Diagnose Problems” on page 5-1.

When the Box Status green LED is on and the yellow LED is blinking, the unit is executing beacon recovery. For more information, see “Beaconing on the Data Network” on page 5-21.

For more information about the Port LEDs, see “Check Port Status” on page 5-39.

For more information about the Ring In/Ring Out Status LEDs, see “Check RI/RO Status” on page 5-40.

For more information about the Data In/Data Out Status LEDs, see “Check DI/DO Status” on page 5-41.

For more information about the Control In/Control Out Status LEDs, see “Check CI/CO Status” on page 5-42.

Beaconing on the Data Network

The 8239 automatically detects and isolates faults that result in hard errors (beaconing) on the network. To determine if beaconing has occurred, see “Check for Hard Errors (Beaconing) on the Data Network” on page 5-31. In the event that the network continues to beacon, see “Isolate Beaconing” on page 5-33.

Soft Errors on the Data Network

Soft errors are usually intermittent faults that temporarily disrupt operation of a token-ring network. When a station inserts into the ring, it is normal for some soft errors to occur. Problems with cabling or with devices on the network may cause soft errors that indicate a problem. An excessive number of soft errors can result in degraded ring performance.

Each station keeps counters associated with the most critical soft errors and reports them by sending out a Report Soft Error MAC Frame. These soft errors are categorized into Isolating Error Counts and Non-Isolating Error Counts:

- Isolating Error Counts include
  - Line error
  - Internal error
  - Burst error
  - A/C error
  - Abort delimiter transmitted
- Non-Isolating Error Counts include
  - Lost frame error
  - Receiver congestion
  - Frame-copied error
  - Frequency error
  - Token error

Note: Ring purge and claim frames are not normally considered soft errors because these conditions are not reported in the Report Soft Error MAC frame. For the purposes of understanding the stability of the network and how it is functioning on a MAC-level basis, purge and claim frames will be discussed along with soft errors.

Unlike hard errors, a device does not normally take any automatic action to isolate and remove the source of soft error faults from the network.

To determine what soft errors are present on the network, see “Check for Soft Errors on the Data Network” on page 5-34. To isolate soft errors, see “Isolate Soft Errors” on page 5-38.

Hub Resets Unexpectedly

When the 8239 detects an unexpected failure condition, it resets itself to automatically recover from the problem. If this reset occurs, record the information obtained through the use of the commands listed below and contact your provider of service.

- DISPLAY STACK
- DISPLAY NETWORK_MAP for all segments in the stack, specifying ALL_STATIONS on an 8239 Model 1 or LOCAL_STATIONS on a Model 2
- DISPLAY MANAGEMENT_INTERFACE for all Model 1s in the stack

- RETRIEVE ERROR_LOG from the hub that reset
- RETRIEVE TRAP_LOG for all hubs in the stack
- RETRIEVE TRACES from all the hubs in the stack

You should also be prepared to provide as many details as possible regarding what occurred before the reset.

Unable to Obtain Information from Other Hubs in the Stack

If you are unable to access another hub in the stack, check for these problems:

- The hub unexpectedly reset. See“Hub Resets Unexpectedly” on page 5-21 .
- The control ring has been segmented. See “Verify the Physical Path Between Hubs” on page 5-46.
- Problems on the control ring are hampering communications between hubs. See “Check for Errors on the Control Ring” on page 5-47.
- A failure has occurred on the hub. See “Check for a Fatal Error on the Hub” on page 5-48.

Note that the DISPLAY STACK terminal interface command is a useful command to issue to determine which hubs are in the stack from the perspective of device management.

Unexpected Hub Down Trap

The 8239 continually makes sure that successful communications exist among the hubs in the stack. Unexpected Hub Down traps can occur for the following reasons:

- The hub reset unexpectedly. See “Hub Resets Unexpectedly” on page 5-21.
- The control ring has been segmented. See “Verify the Physical Path Between Hubs” on page 5-46.
- Problems on the control ring are hampering communications between hubs. See “Check for Errors on the Control Ring” on page 5-47.
- A failure has occurred on the hub. See “Check for a Fatal Error on the Hub” on page 5-48.

Note that the DISPLAY STACK terminal interface command is a useful command to issue to determine which hubs are in the stack from the perspective of device management.

Code Version Mismatch Trap

A code version mismatch trap indicates that all of the hubs in the stack are not running the same version of operational code. It is recommended that all hubs in the stack execute the same version of code; otherwise, unpredictable results can occur. To insure that all hubs are running the same level of code, perform one of these steps:

- If one of the 8239 Model 1s in the stack is currently executing the desired version of code, issue the REPLICATE OPERATIONAL_CODE terminal interface command to that Model 1. The Model 1 will update all of the hubs in the stack (Model 1s and Model 2s) with the version of code that it is running. After the command completes successfully, issue RESET_HUB for all of the hubs in the stack that were not already running the appropriate version of code.
- If there is not an 8239 Model 1 in the stack that is currently executing the desired version of code, issue LOAD OPERATIONAL_CODE to load the

appropriate version of code on the hub. After the command completes successfully, issue RESET_HUB for all of the hubs in the stack that were not already running the appropriate version of code; this step will execute the new code. For more information about updating code, see “Updating 8239 Operational Code” on page 7-3.

Station Is Not Listed in the Network_Map

When a station is known to be inserted into the network (see “Check Port Status” on page 5-39 for information about stations locally attached to the 8239) , the following reasons could explain why the station may not be properly listed when a DISPLAY NETWORK_MAP terminal interface command is issued:

- The station is inserted, but the physical configuration of the network is not correct. See “Verify that a Physical Path Exists Between Two End Stations” on page 5-30.
- If the station is not locally attached to the 8239, then the following conditions must exist for the station to appear in the network _map:
  - An 8239 Model 1 with its RMON Ring Station group enabled is inserted on the segment. To verify that the ring station group is enabled, see “Check the RMON Group Status” on page 5-48. To verify that the Model 1 is inserted on the segment, see “Verify that the Management Interface is Inserted” on page 5-25.
  - DISPLAY NETWORK_MAP ALL_STATIONS is used to display the network_map.
  - The RMON Ring Station table is full. See “Expected Entry is not Reported by RMON.”

  Be aware that a station can be temporaily listed as *external* due to timing differences between the Model 1’s RMON function and address-to-port mapping function.
- Errors on the ring that prevent the Neighbor Notification Process from completing successfully. See “Check the Neighbor Notification Process” on page 5-45.
- The station is attached to a fanout device that is locally attached to the hub and there are more than 8 stations connected to this fanout device. In this situation, the 9th to *n*th stations will not be listed unless an 8239 Model 1 with RMON Ring Station group enabled is on the ring, in which case the 9th to *n*th stations will be identified as *external*.
- If multiple fanout devices are attached to consecutive active ports on the same hub and the last station on the first fanout device is changed so that it is the first station on the next fanout device, the mapping facility will not detect the change. The station will still appear in the network_map, but its port number may be incorrect.

Expected Entry is not Reported by RMON

This section applies only to the 8239 Model 1.

Possible reasons that an expected entry is not reported by the 8239's RMON agent are:

- The Management Interface is not inserted into the network. See “Verify that the Management Interface is Inserted” on page 5-25.

- The RMON Group is disabled. See “Check the RMON Group Status” on page 5-48.
- The RMON table is full. See “Clearing or Deleting an RMON Table” on page 5-48.
- The RMON Ring Station table may not be accurate if there are problems on the network that prevent the Neighbor Notification Process from completing successfully. See “Check the Neighbor Notification Process” on page 5-45.

Expected Data is not Displayed on Nways RMON Manager

If you are using an RMON Manager (for example, Nways Workgroup Remote Monitor or Nways Manager Remote Monitor) and the RMON data or panels are not being displayed as expected, follow these steps:

- Refresh the view.
- Make sure that an interface description is displayed when the device (probe) is selected. If it is not displayed, you may have a connectivity problem. See “Unable to Communicate with the Management Interface” on page 5-18.
- Make sure that the community name for the device is correct by checking the device or probe configuration on your RMON Manager. A community name of *public* is too low an access level to permit the drawing of screens on the Nway RMON Manager application.
- Make sure the appropriate RMON groups are enabled. See “Check the RMON Group Status” on page 5-48.

CRS Data is not Available

This section applies only to the 8239 Model 1.

When the Configuration Report Server (CRS) surrogate agent on the 8239 Model 1 is active, it sends CRS Request MAC frames to all stations participating in the Neighbor Notification Process every 10 minutes and after NAUN changes occur. If a station does not respond to the CRS Request frame, the 8239 sends out the CRS Request MAC frames every minute. Use the DISPLAY TR_SURROGATE CRS_STATION ALL terminal interface command to identify the MAC address that did not respond and take action.

Any errors on the ring may also affect the ability of CRS to gather its data. See “Check for Hard Errors (Beaconing) on the Data Network” on page 5-31 and “Check for Soft Errors on the Data Network” on page 5-34.

Additional Procedures

General Information about the 8239

It is useful to obtain certain 8239 information before beginning problem determination or calling your provider of service. To obtain this information, issue the following terminal interface commands:

- DISPLAY STACK
- DISPLAY NETWORK_MAP for all segments in the stack, specifying ALL_STATIONS on an 8239 Model 1 or LOCAL_STATIONS on a Model 2
- DISPLAY PORT ALL
- DISPLAY MANAGEMENT_INTERFACE for all Model 1s in the stack

- RETRIEVE ERROR_LOG for all hubs in the stack
- RETRIEVE TRACES for all hubs in the stack
- RETRIEVE TRAP_LOG for all hubs in the stack

Verify Management Interface Configuration for Connectivity

In order to have in-band connectivity to the 8239 Model 1's Management Interface, the Model 1 must be configured properly with IP information. To verify that the IP information is correct, issue the DISPLAY IP terminal interface command to the Model 1. If the information is incorrect, issue SET IP.

The Management Interface defaults to setting the source routing bit in ARP Requests. If the 8239 is connected to a network that contains devices (like routers) that do not support source routing, the 8239 needs to be configured so that the source routing bit is not set in ARP Requests. To determine the current configuration for the 8239, issue DISPLAY MANAGEMENT_INTERFACE and find the value displayed for ARP Resolve Method. To configure the 8239 so that the source routing bit is not set, issue SET MANAGEMENT_INTERFACE ARP_RESOLVE_METHOD DISABLE.

Verify that the Management Interface is Inserted

In order to communicate with the 8239 Model 1 using in-band connectivity, the Model 1's Management Interface must be inserted into the data network. To verify that the Management Interface is inserted into the data network using the terminal interface, issue the DISPLAY MANAGEMENT_INTERFACE terminal interface command. For the Management Interface to be inserted into the data network, the results of the DISPLAY command should indicate that:

- Administrative Mode is ENABLED
- Adapter Status is OPENED
- Diagnostics Wrap Mode is NONE

To verify that the Management Interface is inserted into the network using the 8239 Model 1 LCD, the management_interface_status field should be either:

- opn
- A hexadecimal number that represents the ring number of the segment

The following chart lists the various states of the Management Interface, explains how to determine the state from the terminal interface or LCD, and gives instructions for inserting the Management Interface into the network. You will probably need to issue any terminal interface commands using the EIA-232 interface since in-band connectivity is not available.

Management Interface State	Result from DISPLAY MANAGEMENT_INTERFACE	LCD management_ interface_status field	Action
Inserted into the network	• Administrative Mode ENABLED • Adapter Status OPENED • Diagnostics Wrap NONE	opn or ring segment number	None
Administratively disabled	Administrative Mode DISABLED	wrp	Issue SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE ENABLE
In diagnostics wrap mode	Diagnostics Wrap is EXTERNAL or INTERNAL	dwr	Issue SET MANAGEMENT_INTERFACE DIAGNOSTICS_WRAP NONE
Cannot insert into the network	• Administrative Mode ENABLED • Adapter Status CLOSED or OPENING • Diagnostics Wrap NONE	cls	See “The Management Interface Cannot Insert” on page 5-27
Beacon wrapped	• Administrative Mode ENABLED • Adapter Status BEACON WRAPPED • Diagnostics Wrap NONE	bwr	No action required. 8239 will automatically try to insert into the network
Exceeded beacon threshold error	• Administrative Mode ENABLED • Adapter Status BEACON_THRES_ERROR • Diagnostics Wrap NONE	ber	To allow the Management Interface to be inserted into the network, issue SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE and then SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE ENABLE. If the Management Interface continues to become beacon wrapped, contact your provider of service.
Reset. The Management Interface did not initialize successfully or encountered a failure	Adapter Status NOT INITIALIZED	rst	Reset the Model 1. If this symptom persists, get the error log information using RETRIEVE ERROR_LOG and contact your provider of service.

The Management Interface Cannot Insert

These conditions can prevent the Management Interface from inserting into the network:

- A problem on the network
- Management Interface configuration problem
- A problem within the 8239

To determine why the Management Interface is unable to insert, issue the DISPLAY COUNTER 802.5 terminal interface command and look at the Ring Open Status (dot5RingOpenStatus in the 802.5 MIB). No configuration changes need to be made to get this information; the 802.5 Interface table is automatically supported and the support cannot be disabled. The following table identifies the possible values for the Ring Open Status and the action to take:

802.5 Ring Open Status	Action
Last open successful	None
Bad Parameter	Verify that the Management Interface configuration parameters are correct, especially the MAC address and MAC address type. Issue DISPLAY MANAGEMENT_INTERFACE to view current settings. Issue SET MANAGEMENT_INTERFACE to make changes.
• Lobe failed • Signal loss • Insertion timeout • Ring failed • Beaconing	See if the Management Interface can open when it is isolated. See "Isolate the Management Interface." If the Management Interface was able to open on its own ring, there may be a problem on the network. To use the Management Interface's capabilities to diagnose the network problem, attempt to insert the Management Interface by wrapping all of the ports so that the Management Interface is the only station on the stack ring. Then follow the directions in these sections: • "Beaconing on the Data Network" on page 5-21 • "Soft Errors on the Data Network" on page 5-21 • "Check the Neighbor Notification Process" on page 5-45 If the Management Interface still is not able to open, the problem is within the 8239. Gather the information described in "General Information about the 8239" on page 5-24 and contact your provider of service.
Duplicate MAC address	Verify that another station is not configured with the same MAC address configured for the Management Interface. Issue DISPLAY MANAGEMENT_INTERFACE to view current settings.
Request failed	Handshaking with the RPS failed. See "Check Station Receiver Congestion on Insert" on page 5-42.

Isolate the Management Interface

Whenever the Management Interface is isolated, it should have no problems inserting into the ring because it is on its own segment. To isolate the Management Interface, issue the SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE terminal interface command. Be aware that once this command is issued, in-band connectivity is lost and SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE and any other 8239 commands must be issued using the EIA-232 interface.

Once the Management Interface's Administrative Mode is disabled, the Management Interface should open within 20 seconds. Issue DISPLAY MANAGEMENT_INTERFACE and the Adapter Status should be OPENED. In addition, since the Management Interface is the only station on the ring, the value of Ring Status should be SINGLE STATION when DISPLAY COUNTER 802.5 is issued.

Check the Management Interface's Receive Capability

If the Management Interface is able to receive frames, then various counters associated with receiving frames will increment. When any RMON group is enabled on the 8239 Model 1 (after a DISPLAY MANAGEMENT_INTERFACE terminal interface command, RMON Mode will be ENABLED), the Management Interface copies all frames on the network. If no RMON groups are enabled, then send traffic directly to the 8239 Model 1 to trigger the Management Interface to receive frames. (For example, issue a ping to the 8239 Model 1's IP address from a station that is on the same segment as the Model 1.) Depending on traffic and the functions that are enabled on a Model 1, the Model 1's Management Interface may not be able to receive or process all frames.

Verifying that the Management Interface is Receiving Frames: The Management Interface has counters that identify how many frames it has received. To see these counters, use one of these methods:

- Issue the DISPLAY COUNTER MIB2_INTERFACE terminal interface command several times and see if the Received Packet counters are incrementing. When any RMON group is enabled, the Received Non-Unicast Packets will automatically increment at least every 7 seconds as a result of successfully receiving the Neighbor Notification MAC frames. If no RMON group is enabled, then any frames directed to the Management Interface's MAC address result in incrementing the Received Non-Unicast Packets counter if the frames were successfully received. Receiving other frames will also result in incrementing the Received Packet counters.
- If the Management Interface's RMON Host Group is enabled, then issue DISPLAY RMON HOST_DATA HOST_ADDRESS several times, specifiying the Management Interface's MAC address; see if the Input Packets counter is incrementing. To determine if the RMON Host Group is enabled, issue DISPLAY RMON GROUP_STATUS. To enable the Host Group, issue ENABLE RMON HOST.

Recovering from Not Receiving Frames: If none of the Management Interface's receive-related counters are incrementing, attempt to recover by causing the Management Interface to change its state, using either of these methods:

- Force the Management Interface to deinsert and then automatically reinsert into the network. Note that this procedure may result in the counters kept by the Management Interface for network monitoring purposes being cleared. To get the Management Interface to deinsert and then reinsert, change the Management Interface's Early Token Release Mode to its opposite state. Determine its current state by issuing DISPLAY MANAGEMENT_INTERFACE. Then, issue SET MANAGEMENT_INTERFACE EARLY_TOKEN_RELEASE for the opposite setting. This method is only applicable if the Management Interface is on a 16-Mbps segment. If the Management Interface is on a 4-Mbps segment, use the Management Interface diagnostics feature to get the Management Interface to change its state; accomplish this by issuing SET

MANAGEMENT_INTERFACE DIAGNOSTIC_WRAP INTERNAL followed by SET MANAGEMENT_INTERFACE DIAGNOSTIC_WRAP NONE. Note that once SET MANAGEMENT_INTERFACE DIAGNOSTIC_WRAP INTERNAL command is issued, in-band connectivity is lost and SET MANAGEMENT_INTERFACE DIAGNOSTIC_WRAP NONE must be issued using the EIA-232 interface.

- Obtain the information described in “General Information about the 8239” on page 5-24. Then reset the 8239 Model 1 by issuing RESET_HUB for the Model 1.

If the Management Interface's receive counters still do not increment, contact your provider of service.

Verifying That the Management Interface Has Receiver Congestion: Even if the Management Interface’s receive counters are incrementing, the Management Interface may still have problems receiving frames. Depending on the amount of network traffic, the amount of data being sent to the 8239 Model 1’s IP address, and the network monitoring functions enabled on the 8239 Model 1, the Model 1 may not be able to receive all of the network traffic; if it cannot keep up, the Management Interface indicates that its receiver is congested by sending out Soft Error Report MAC frames with a receiver congestion counter that is non-zero. To determine whether the Management Interface is experiencing receiver congestion, use one of these methods:

- If the Management Interface's 802.5 group is enabled, issue DISPLAY COUNTER 802.5 several times; see if the Receive Congestions counter is incrementing. To determine the status of the 802.5 group, issue DISPLAY MANAGEMENT_INTEFACE and look for the value of 802.5 Group. If it is disabled, issue SET MANAGEMENT_INTERFACE 802.5_GROUP ENABLE to enable it.
- If the Management Interface’s RMON Ring Station Group is enabled, issue DISPLAY RMON RING_STATION_DATA HOST_ADDRESS several times, specifiying the Management Interface’s MAC address; verify whether the Congestion Errors counter is incrementing. To determine whether the RMON Ring Station Group is enabled, issue DISPLAY RMON GROUP_STATUS. To enable the Ring Station Group, issue ENABLE RMON RINGSTATION.

Verifing that the Management Interface is Dropping Frames: The Management Interface automatically detects when its receiver is nearly congested and it is unable to keep up with network traffic. To keep this condition from affecting connectivity to the hub, the Management Interface will continue processing all frames received that are destined for it, but there will be no RMON processing performed on any LLC frames received, whether the LLC frames are destined for the Management Interface or not. While in this state, RMON data reported for LLC frames will not be accurate. The Management Interface automatically resumes RMON processing for LLC frames when receive buffers are available.

When the Management Interface receives a frame but does no RMON processing on it, the RMON 2 MAC Layer Statistics Dropped Frames counter is incremented.

There is no terminal interface support to access this counter. You can query this counter only using SNMP[1].

Recovering from Receiver Congestion: If the Management Interface is experiencing receiver congestion, you can use these steps to minimize the receiver congestion:

- Disable any unnecessary network monitoring functions on the 8239 Model 1 to reduce the load on the Model 1.
- Have more than one Model 1 in the stack connected to the same segment so that the Model 1 functions can be distributed across multiple Model 1s. For example, one Model 1 can have RMON enabled but not be used for device management, while another Model 1 is used for device management and all of its RMON groups are disabled.

Check the Management Interface's Transmit Capability

The Management Interface can be triggered to send data by issuing the PING terminal interface command. You can then verify whether the Management Interface is able to transmit frames by accessing 8239 information. Issue PING for an operational station whose MAC address is not currently in the 8239's ARP cache. After PING is issued, follow these steps:

1. Issue DISPLAY ARP_CACHE. If an ARP cache entry exists and the MAC address for the station is identified, then the Management Interface's transmit path is operational. Other problems can prevent your receiving ping replies.
2. Issue DISPLAY COUNTER MIB2_INTERFACE and you should see that either:
   - The Transmitted Non-Unicast Packets counter has increased by at least 10 if there is no response to the ping.
   - The Transmitted Unicast Packets counter increased by at least 10 if there is a response to the ping.

   Note that the counter can increase by more than 10 if the 8239 is sending out other frames besides the ping. If one of the Transmitted Packets counters does not increase by at least 10, contact your provider of service.

Verify that a Physical Path Exists Between Two End Stations

In order for two stations (a work station or the Management Interface) to communicate with each other, either they must be on the same local segment or the segments must be connected through an external device, such as a bridge or router. To verify that there is no problem with the physical path between the two stations from the perspective of the 8239:

1. Verify that the stations are inserted into the network. If the stations are locally attached to the 8239, verify that the stations are inserted into the network. For infomation on how to verify that the stations are inserted, see "Check Port Status" on page 5-39.
2. Verify that the data path exists for connectivity.

---

[1] Nways Workgroup Remote Monitor for Windows NT Version 1.1 does not contain support for querying the RMON 2 Dropped Frames counter. If your RMON Management application does not have this support, you can use a MIB Browser that has the RMON-2 MIB. The MIB Object ID is `internet.mgmt.mib-2.rmon.statistics.tokenRingMLStats2Table.tokenRingMLStats2Entry.tokenRingMLStatsDroppedFrames`.

a. If one of the stations is attached to a hub that is connected to an 8239 Model 1 RI/RO Module, then verify that the RI/RO path is OK. On a DISPLAY RING_IO terminal interface command, the RI and RO administrative mode should be ENABLED and the status should be UNWRAPPED. If the administrative mode is DISABLED, then issue ENABLE RING_IO to enable it. If the status is WRAPPED, there may be a problem with the segment connected to the external device.

   Note: If there are multiple RI/RO connections between two ring segments, make sure that multiple independent segments have not been inadvertently created.

b. Verify that all of the data connections in the 8239 for this segment are OK. For each of the hubs on the desired segment, issue DISPLAY WRAP_POINTS and verify that the appropriate Data In and Data Out wrap points are unwrapped. If any of them are inappropriately wrapped, issue UNWRAP DATA_IO for the appropriate wrap point. Note that segmenting the 8239 stack into multiple data segments can cause the data path between stations to cease to exist; the station may need to be moved to a different hub.

c. Verify that all of the port hardware connections in the 8239 for this segment are OK. For each of the hubs on the desired segment, issue DISPLAY WRAP_POINTS and verify that the Port Isolate, Main Port and Expansion Port wrap points have a value of UNWRAPPED. If any of them have a value of WRAPPED, then issue UNWRAP PORTS_IO for the appropriate wrap point.

If there is no problem with the data path within the 8239, then there may be a problem with the data path in a different part of the network or there may be a problem with the network itself. The complete network data path can be confirmed as fully operational if connectivity exists (for example, ping completes successfully) between two additional stations that are known to communicate with other stations and are attached to the same devices as the original stations.

Check for Hard Errors (Beaconing) on the Data Network

The 8239 Model 1 supports functions that allow you to proactively monitor the network for beaconing and inform you, realtime, when they occur. This section describes methods of monitoring and obtaining information about beaconing conditions.

The 8239 beacon recovery function is continuously running to detect and isolate beaconing faults. This continuous running of the function can result in the 8239 Model 1's Management Interface not seeing all frames on the network if the 8239 beacon recovery algorithm temporarily wraps the Management Interface.

Using REM to Detect Beaconing: To be informed when beaconing occurs on the network, use the 8239 Model 1's Ring Error Monitor (REM) function. REM can be configured to send a trap when beaconing occurs on the network and it will also send traps on the status of the beaconing. If you are concerned about beaconing on your network, it is recommended that you enable REM to send traps as part of normal operations. The following table identifies what needs to be configured, how to determine the current configuration settings, and how to enable the settings. The default setting is DISABLED for everything except for the REM Trap Flag.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Surrogate Function	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN SURR_STATUS
REM Group	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN REM_STATUS
REM Trap Flag to receive any REM trap generated (see note)	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS REM_TRAPS

Note: When a REM trap is generated, it is automatically put in the trap_log (DISPLAY TRAP_LOG terminal interface command). It will also be displayed on the terminal interface as long as the CONSOLE_DISPLAY trap_setting is enabled (to see the current setting, issue DISPLAY TRAP_SETTINGS). To send the trap to an SNMP trap receiver, an entry is required in the trap community table. To add an entry, issue SET TRAP_COMMUNITY TR_SURROGATE. To see the current entries, issue DISPLAY COMMUNITY.

To obtain information about the last beacon frame seen on the network by the Management Interface, issue the DISPLAY TR_SURROGATE REM_LAST_BEACON terminal interface command.

Using RMON to Detect Beaconing: RMON Alarms and Events, along with the RMON MAC-layer Statistics group, can also be used to send a trap when a configured alarm occurs. Unlike REM, you must configure the specific characteristics of the alarm to trigger the event. The following table identifies what you need to enable on the 8239 Model 1 in order to set up the alarm on a specific beacon condition. The default setting is ENABLED for all of the groups.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
RMON MAC-layer Statistics group	DISPLAY RMON GROUP_STATUS	ENABLE RMON MAC_LAYER
RMON Alarm group	DISPLAY RMON GROUP_STATUS	ENABLE RMON ALARM
RMON Event group	DISPLAY RMON GROUP_STATUS	ENABLE RMON EVENT

To set up the event and alarm, use an RMON Manager, such as the IBM Nways Workgroup Remote Monitor; it provides a graphical interface. You also can set up the event and alarm using the terminal interface by issuing the following commands:

1. SET RMON EVENT LOG_TRAP or SET RMON EVENT TRAP
2. SET RMON ALARM MLSTATS

To obtain the number of hard errors that occur over time, use the RMON History Group to gather MAC-layer statistics. Relevant terminal interface commands are SET RMON HISTORY_CONTROL, DISPLAY RMON CONTROL HISTORY, and DISPLAY RMON HISTORY_ML_DATA. To view a summary of the latest beacon statistics, issue DISPLAY RMON STATISTICS_DATA MAC_LAYER.

Querying 8239 Status for Beacon Conditions: When beaconing occurs and the 8239 isolates the beacon fault by wrapping it out of the network to minimize the impact to the rest of the network, the 8239 identifies the entity that was wrapped as BEACON WRAPPED or BEACON THRES ERROR. The following table identifies the entities that the 8239 can beacon wrap and the teminal interface command that allows you to determine the status.

Potential Beacon Fault Areas	Commands to Display Status
Management Interface (Model 1 only)	• DISPLAY MANAGEMENT_INTERFACE • DISPLAY WRAP_POINTS
Port	DISPLAY PORT
Data In/Data Out	DISPLAY WRAP_POINTS
Ring In/Ring Out (Model 1 only)	DISPLAY RING_IO

Using 8239 Traps for Notification of Beacon Faults: Except for the Management Interface, a trap is generated whenever the 8239 performs a beacon wrap. To generate the trap[2], the 8239 must be configured properly. The following table identifies what you need to configure, how to determine the current configuration settings, and how to enable the parameter. The default setting is ENABLED for everything.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Management Interface (Model 1 only)	Not available	Not available
Port	DISPLAY TRAP_SETTINGS and DISPLAY PORT	ENABLE TRAP_SETTING PORT_UP_DOWN and ENABLE PORT_SETTING TRAPS
Data In/Data Out	DISPLAY TRAP_SETTINGS	ENABLE TRAP_SETTING DATA_IO_STATUS_UP_DOWN
Ring In/Ring Out (Model 1 only)	DISPLAY TRAP_SETTINGS	ENABLE TRAP_SETTING RING_IO_STATUS_UP_DOWN

Isolate Beaconing

The 8239 should automatically isolate beaconing faults on the network. In the event that it does not automatically isolate faults, refer to the *Token-Ring Problem Determination Guide*, SX27–3710, for information about beacon recovery and beacon isolation. Follow the steps identified for the IBM 8228 or IBM 8230.

The 8239 address-to-port mapping information obtained by issuing DISPLAY NETWORK_MAP may be useful in understanding the network configuration and potential fault domains.

---

[2] When an 8239 private trap is generated, it is automatically put in the trap_log (view the trap log using DISPLAY TRAP_LOG). The trap is also displayed on the terminal interface as long as the CONSOLE_DISPLAY trap_setting is enabled (issue DISPLAY TRAP_SETTINGS to view the current setting). To send the trap to an SNMP trap receiver, an entry is required in the trap community table. To add an entry, issue SET TRAP_COMMUNITY IBM8239. To view the current entries, issue DISPLAY COMMUNITY.

For assistance with isolating the fault by simplifying the configuration see "Segmenting to Isolate Problems" on page 5-38.

Check for Soft Errors on the Data Network

Unless you use a tool to help you identify when soft errors are on the network, the occurrence of soft errors usually is undetected until a user complains that he is having problems communicating with a server or station. The 8239 Model 1 supports functions that allow you to monitor the network for soft errors, inform you, realtime, when they occur, or identify the potential fault domain of the error. This section describes methods of monitoring soft errors and what to do when they occur. Note that soft errors and ring purges are normal occurrences on the network when stations enter the ring or there is a ring reconfiguration, even if the 8239's purge-on-insert function is disabled

Using REM to Detect Soft Errors: To be informed when stations report occurrences of soft errors in the Report Soft Error MAC Frame, use the 8239 Model 1's Ring Error Monitor (REM) function. REM can be configured to send a trap when any Report Soft Error MAC Frame is sent on the ring or it can be configured to notify you when excessive soft error conditions may be present that warrant further investigation. The trap contains the soft error condition that occurred, the reporting ring station's MAC address, and its NAUN.

If you are concerned about soft errors on your network, enable the various REM "Exceeded Traps" to allow REM to inform you of potential problems on the network or to give you advance notice of a potential problem. IBM's REM function contains a proprietary algorithm that takes into account various factors, such as the number of soft errors reported, the frequency of occurrence between soft errors, and the fault domain of the soft error. The following table identifies what needs to be configured, how to determine the current configuration settings, and how to enable the parameters. The default setting is DISABLED for all parameters except for REM Trap Flag.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Surrogate Function	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN SURR_STATUS
REM group	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN REM_STATUS
REM Trap Flag to get any REM trap generated (see note)	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS REM_TRAPS
REM trap when an impending soft-error threshold has been exceeded by a particular fault domain	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS WEIGHT_EXCDED_TRAPS
REM trap when an excessive soft-error threshold has been exceeded by a particular fault domain	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS PREWEIGHT_EXCDED_TRAPS
REM trap when a non-isolating soft-error threshold has been exceeded by a particular fault domain	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS NON_ISO_THRESHOLD_EXCDED_TRAPS

Note: When a REM trap is generated, it is automatically put in the trap_log (viewed using DISPLAY TRAP_LOG). It will also be displayed on the terminal interface as long as the CONSOLE_DISPLAY trap_setting is enabled (use DISPLAY TRAP_SETTINGS to see the current setting). To send the trap to an SNMP trap receiver, an entry is required in the trap community table. To add an entry, issue SET TRAP_COMMUNITY TR_SURROGATE. To see the current entries, issue DISPLAY COMMUNITY.

When a station is in the pre-weight exceeded or weight exceeded condition and you need to be informed whenever the specific soft error counter is non-zero, enable the appropriate auto-intensive flag associated with the desired soft error counter in order to generate the Forward Soft Error MAC Frame trap; the “Exceeded Trap Flags” do not need to be enabled. The following table identifies the minimum action required for the 8239 Model 1 to generate the Forward Soft Error MAC frame trap when the appropriate network conditions exist.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Surrogate Function	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN SURR_STATUS
REM group	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN REM_STATUS
REM Trap Flag to get any REM trap generated (see note)	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS REM_TRAPS
Appropriate auto-intensive flag for a particular soft error counter.	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS AUTO_*_DATA, where * is the text associated with the soft error counter

Note: When a REM trap is generated, it is automatically put in the trap_log (viewed using DISPLAY TRAP_LOG). It will also be displayed on the terminal interface as long as the CONSOLE_DISPLAY trap_setting is enabled (use DISPLAY TRAP_SETTINGS to see the current setting). To send the trap to an SNMP trap receiver, an entry is required in the trap community table. To add an entry, issue SET TRAP_COMMUNITY TR_SURROGATE. To see the current entries, issue DISPLAY COMMUNITY.

When you are experiencing a specific problem that causes you to want to be informed every time a specific soft error counter is non-zero, enable the appropriate auto-intensive flag associated with the desired soft error counter; this action will cause the generation of the Forward Soft Error MAC Frame. Note that excessive traps may be generated. The following table identifies the minimum actions to cause the 8239 Model 1 to generate the Forward Soft Error MAC frame trap whenever a counter is non-zero in a Report Soft Error MAC frame.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Surrogate Function	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN SURR_STATUS
REM group	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN REM_STATUS
REM Trap Flag to get any REM trap generated (see note)	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS REM_TRAPS
Appropriate auto-intensive flag for a particular soft error counter (see note).	DISPLAY TR_SURROGATE REM_STATUS	ENABLE TR_SURROGATE REM_STATUS RING_*_DATA, where * is the text associated with the soft error counter

Note: When a REM trap is generated, it is automatically put in the trap_log (viewed using DISPLAY TRAP_LOG). It will also be displayed on the terminal interface as long as the CONSOLE_DISPLAY trap_setting is enabled (use DISPLAY TRAP_SETTINGS to see the current setting). To

send the trap to an SNMP trap receiver, an entry is required in the trap community table. To add an entry, issue SET TRAP_COMMUNITY TR_SURROGATE. To see the current entries, issue DISPLAY COMMUNITY.

To obtain the soft error statistics maintained by REM, issue the appropriate terminal interface command:

- DISPLAY TR_SURROGATE REM_ISOLATING
- DISPLAY TR_SURROGATE REM_LAST_SOFT_ERROR
- DISPLAY TR_SURROGATE REM_NONISO_THRESHOLD_EXCD
- DISPLAY TR_SURROGATE REM_NONISO_SOFT_ERROR

Using RMON to Detect Soft Errors: RMON Alarms and Events, along with the RMON MAC-layer Statistics group, can also be used to send a trap when a configured alarm occurs. Unlike REM, you must configure the specific characteristics of the alarm to trigger the event. The alarm characteristics should take into account your normal traffic patterns to avoid triggering the alarm prematurely. The following table identifies what needs to be enabled on the 8239 Model 1 in order to set up the alarm on a specific soft error condition. The default setting is ENABLED for all of the groups.

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
RMON MAC-layer Statistics group	DISPLAY RMON GROUP_STATUS	ENABLE RMON MAC-LAYER
RMON Alarm group	DISPLAY RMON GROUP_STATUS	ENABLE RMON ALARM
RMON Event Group	DISPLAY RMON GROUP_STATUS	ENABLE RMON EVENT

To set up the event and alarm, it is recommended that you use an RMON Manager, such as the IBM Nways Workgroup Remote Monitor, because they provide an easy-to-use graphical interface. You can also set up the event and alarm using the terminal interface by issuing the following commands:

1. SET RMON EVENT LOG_TRAP or SET RMON EVENT TRAP
2. SET RMON ALARM MLSTATS

To obtain the number of soft errors that occur over time, use the RMON History Group to gather MAC-layer statistics. Relevant terminal interface commands are:

- SET RMON HISTORY_CONTROL
- DISPLAY RMON CONTROL HISTORY
- DISPLAY RMON HISTORY_ML_DATA

To view a summary of the latest soft error statistics, issue the DISPLAY RMON STATISTICS_DATA MAC_LAYER terminal interface command.

Detecting Ring Purges or Claim Frames: REM does not monitor ring purge or claim frames. Thus, RMON is the best methods of determining when excessive ring purges or claim frames are on the network; use the instructions in “Using RMON to Detect Soft Errors.” When setting up the alarm, specify any of the following parameters instead of a soft error counter:

- RING_PURGE_EVENTS
- RING_PURGE_PACKETS
- CLAIM_TOKEN_EVENTS

- CLAIM_TOKEN_PACKETS

Isolate Soft Errors

Isolating soft errors can be a difficult process, especially when the soft errors are non-isolating. It is often a trial-and-error process. Refer to the *Token-Ring Problem Determination Guide*, (SX27-3710) for information about diagnosing soft errors and isolating soft error faults. Follow the steps identified for the IBM 8228 or IBM 8230.

The 8239 address-to-port mapping information obtained by issuing the DISPLAY NETWORK_MAP terminal interface command may be useful in understanding the network configuration and potential fault domains.

For assistance in isolating the fault by simplifying the configuration, see "Segmenting to Isolate Problems." If one or more stations are identified to be the fault, see "Remove a Station" on page 5-46 .

Segmenting to Isolate Problems

The 8239 contains hardware wrap points that can be used to segment various portions of the 8239 for use in problem determination. See Appendix B, "Wrap Point References" on page B-1 for a diagram of the wrap points within the 8239. Note that wrapping any of these points alters the configuration of your network and can cause connectivity problems.

The following table identifies the wrap points, the default settings for normal operations, and the command needed to change the settings. To display the current settings, issue the DISPLAY WRAP_POINTS terminal interface command.

Wrap Point	Default Setting	Terminal Interface Command to Force a Wrap
Management Interface (Model 1 only)	Unwrapped	SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE
Port Isolate (wrap all ports from the stack ring)	Unwrapped	WRAP PORTS_IO ISOLATE
Ports Main (wrap ports 1-16 from the stack ring)	Unwrapped	WRAP PORTS_IO MAIN
Port Expansion (wrap ports 17-32 from the stack ring)	Unwrapped	WRAP PORTS_IO EXPANSION
Data In/Data Out	Unwrapped for a single data segment in the stack	WRAP DATA_IO
Ring In/Ring Out (Model 1 only)	Wrapped	WRAP RING_IO

Note: When using in-band connectivity, any changes to wrap points could disrupt the ability to communicate with the Management Interface.

When segmenting within the 8239 to isolate the fault, it is recommended that you simplify the configuration starting outward and moving inward. For example:

1. Wrap RI and RO.
2. If the problem persists, wrap DI and DO.
3. If the problem persists, move to the ports.
4. Wrap the Management Interface last, especially if in-band connectivity is being used to issue the commands.

Check Port Status

This procedure identifies the possible states of a port, what it means to be in these states, and what action to take for each state. To determine the status of the port that a station is attached to, use one of the following methods:

- If the station has recently tried to insert, display the trap log using the DISPLAY TRAP_LOG terminal interface command and look for any Port Up/Down Traps. To view these traps, you must configure the following flags:
  - The global Port Up/Down trap_setting flag – Issue DISPLAY TRAP_SETTINGS to view the current value and ENABLE TRAP_SETTINGS PORT_UP_DOWN to enable the flag.
  - The Port trap flag associated with a specific port – Issue DISPLAY PORT to see the current value and ENABLE PORT_SETTINGS TRAPS to enable the flag.
- Look at the Port LEDs on the front panel of the 8239 and see “Port Status” on page 5-3.
- Issue the DISPLAY PORT terminal interface command and use the table below to determine the proper action.

Port Status	Description	Action
Inserted	The device connected to this port is successfully inserted into the network.	None
No Phantom	The station did not raise phantom.	If the device connected to the NIC does not present phantom voltage, then the port must be configured for 8228 mode in order to be inserted. Issue DISPLAY PORT to view the current value and issue ENABLE PORT_SETTINGS TRAPS to enable the flag. If the flag already is enabled, verify that the station is operating properly and that the cables connecting the station to the hub are OK.
Security Breach	A MAC address that is not in the port's security table was inserted.	If it is OK for that workstation to be inserted at that port, add the station's MAC address to the port's security table by issuing SET SECURITY_PORT MAC _ADDRESS.
Speed Mismatch	A station entered the ring at the wrong speed.	Make sure the station is configured with the same ring speed as the 8239.
BCN THRES ERROR	A workstation has exceeded the configured threshold for beacon faults. Issue DISPLAY HUB to view the current value of the threshold; use SET HUB BEACON_THRESHOLD to change it.	Fix the beaconing condition and then allow the station to be inserted into the network by issuing ENABLE PORT. To determine if the beaconing fault is in the adapter or the cable, run the diagnostics for your token-ring adapter.
SPD THRES ERROR	A station has exceeded the configured threshold for entering at the wrong speed. Issue DISPLAY HUB to view the current value of the threshold; use SET HUB SPEED_THRESHOLD to change it.	Fix the ring speed configured in the station's token-ring adapter; then allow the station to be inserted into the network by issuing ENABLE PORT.
Beacon Wrapped	A station caused a beacon fault when entering the ring.	Make sure that the cable length and specification comply with the 8239 requirements. Make sure that the station is installed and operating properly by running diagnostics on the station's token-ring adapter.
PHANTOM	The administrative state of this port is disabled.	Use the ENABLE PORT command to allow the hub to insert this port.

Check RI/RO Status

This procedure identifies the possible states for the Ring In and Ring Out connections, the meaning of each state, and what action is required. This section applies only to the 8239 Model 1 when a RI/RO Module is present. To determine the status of the RI/RO connection, use one of the following methods:

- If the station has tried recently to insert, display the trap log using the DISPLAY TRAP_LOG terminal interface command and look for any Ring IO Status Up/Down Traps. For these traps to be recorded, the Ring IO Status Up/Down trap_setting flag must be enabled. To view the current value, issue DISPLAY TRAP_SETTINGS; issue ENABLE TRAP_SETTINGS RING_IO_STATUS_UP_DOWN to enable the flag.

- Look at the RI/RO Status LEDs on the front panel of the 8239 and use “RI/RO Status” on page 5-6 to interpret them.
- Issue DISPLAY RING_IO or DISPLAY WRAP_POINTS and use the table below to determine the proper action.

  Note: Both the DISPLAY RING_IO and DISPLAY WRAP_POINTS commands can be used to determine the status of the RI/RO connection. The advantage of using DISPLAY RING_IO is that this command also displays the RI/RO administrative mode.

RING-IO Status	WRAP_POINTS Status	Description	Action
UNWRAPPED	Unwrapped	The RI or RO connection is inserted into the network.	None.
Wrapped	Wrapped	The RI or RO connection is not inserted into the network.	If the RI/RO administrative mode is disabled, enable it using ENABLE RING_IO. Othewise, make sure that the external device and the cable to the external device are working properly. The 8239 will automatically unwrap RI/RO when the fault is removed.
BEACON WRAPPED	Beacon Wrapped	Beaconing occurred on the segment connected to the external device.	Make sure that the external device and the cable to the external device are working properly. The 8239 will automatically unwrap RI/RO when the fault is removed.

Check DI/DO Status

This procedure identifies the possible states of the Data In and Data Out connections, the meaning of each state, and the action required. DI/DO is used for the data network. To determine the status of the DI/DO connection, use one of the following methods:

- If the station has tried recently to insert, display the trap log using the DISPLAY TRAP_LOG terminal interface command and look for any Data IO Status Up/Down Traps. For these traps to be recorded, the Data IO Status Up/Down trap_setting flag must be enabled. To see the current value, issue DISPLAY TRAP_SETTINGS; issue ENABLE TRAP_SETTINGS DATA_IO_STATUS_UP_DOWN to enable the flag.
- Look at the DI/DO Status LEDs on the front panel of the 8239 and use “Stack In/Stack Out Status” on page 5-7 to interpret them.
- Issue DISPLAY RING_IO or DISPLAY WRAP_POINTS and use the table below to determine the proper action.

WRAP_POINTS Status	Description	Action
Unwrapped	The DI or DO connection is inserted into the network.	None
Wrapped	The DI or DO connection is not inserted into the network.	If the connection needs to be unwrapped, issue UNWRAP DATA_IO.
BEACON WRAPPED	Beaconing occurred off the segment connected to the DI/DO.	Make sure that the stack cable is working properly. The connection will automatically unwrap when the fault is removed. If the symptom persists, the 8239 that this hub is connected to may be faulty; contact your provider of service.

Check CI/CO Status

This procedure identifies the possible states of the Control In and Control Out connections, the meaning of each state, and the action required. The CI/CO is used for the control network, which is the network used between the 8239s to send messages to each other. To determine the status of the CI/CO connection, use one of the following methods:

- If the station has tried recently to insert, display the trap log using the DISPLAY TRAP_LOG terminal interface command and look for any Control IO Status Up/Down Traps. For these traps to be recorded, the Control IO Status Up/Down trap_setting flag must be enabled. To see the current value, issue DISPLAY TRAP_SETTINGS; issue ENABLE TRAP_SETTINGS CONTROL_IO_STATUS_UP_DOWN to enable the flag.
- Look at the CI/CO Status LEDs on the front panel of the 8239 and use “Stack In/Stack Out Status” on page 5-7 to interpret them.
- Issue DISPLAY WRAP_POINTS and use the table below to determine the proper action.

WRAP_POINTS Status	Description	Action
Unwrapped	The CI or CO connection is inserted into the network.	Make sure that the control ring’s MAC interface is opened. See “Verify that the Control Interface MAC is Inserted” on page 5-46.
Wrapped	The CI or CO connection is not inserted into the network.	If the connection should be unwrapped, issue UNWRAP CONTROL_IO.
BEACON WRAPPED	Beaconing occurred off the segment connected to the CI/CO.	Make sure that the stack cable is working properly. The connection will automatically unwrap when the fault is removed. If the symptom persists, the 8239 that this hub is connected to may be faulty; contact your provider of service.

Check Station Receiver Congestion on Insert

Some stations’ adapters are unable to complete the open-adapter insertion process because the adapters experience receiver congestion if there is too much broadcast traffic on the network. If there is a Ring Parameter Server (RPS) on the network and the RPS does not send the Initialize Ring Station Response MAC

frame using express buffering, the adapter may not be able to receive the RPS's response in order to complete the open adapter insertion process.

Note: The 8239 RPS function uses express buffering for the Initialize Ring Station Response MAC frame.

The RPS itself may also be too congested to process the station's Initialize Ring Station Request.

To identify whether the station is unable to complete its open adapter insertion process due to receiver congestion, obtain a network trace that contains the frames on the ring when the station is trying to insert. You can obtain this trace using the 8239's RMON packet capture and filter function or by using an external network analyzer. If you use the 8239's RMON packet capture and filter function, configure the RMON Manager to filter on any broadcast frames and frames sent to or from the station's MAC address. If receiver congestion is the problem, you will observe the following events in the network trace:

- Broadcast frames during the time that the station is trying to insert
- A Soft Error Report MAC frame from the station with a non-zero value in the receiver congestion byte of the Non-Isolating Error Counts
- Address-Recognized bits in the Initialize Ring Station Response MAC frame set to 1 and the Frame-Copied bits set to 0. This event is applicable only if the entity taking the network trace is downstream of the station trying to insert and upstream of the RPS.

See "Check the Receive Capability of the Station" for additional methods of identifying whether the station is experiencing receiver congestion.

If the station is unable to insert into the network due to receiver congestion, try any of these actions:

- Increase the number of receive buffers configured for the station's token-ring adapter.
- If the hub's purge-on-insert configuration option is disabled, enable it. When this option is enabled, the 8239 causes a purge frame to be sent by the Active Monitor after the station requests insertion; the purge frame clears the adapter's receive buffers. The default setting is enabled. To see the current setting, issue the DISPLAY HUB terminal interface command and look at the value for "Purge On Insert". To enable this function, issue ENABLE PURGE_ON_INSERT.
- Disable the port while the station is trying to insert using DISABLE PORT; then enable the port after the station has completed its open-adapter insertion process using ENABLE PORT.

Check the Receive Capability of the Station

When a station is inserted into the network and data is being sent to it, the station should be receiving the frames. The station may not be able to receive the frames if there is a problem with the network or with the station. Methods that can be used to determine if the station should be or is receiving frames are:

- If the 8239's RMON Host group is enabled, issue the DISPLAY RMON HOST_DATA HOST_ADDRESS terminal interface command, specifying the MAC address of the desired station. If the value displayed for Input Packets is non-zero and incrementing, the station should be receiving the frame.

- If the 8239's RMON Promiscuous or Host group is enabled, use an RMON manager to set up a packet capture and filter for any frames destined for the station's MAC address or use an external network analyzer. If the station is able to receive the frames, the Address-Recognized bits in the frames are set to 1 and the Frame-Copied bits are set to 1. This action is only applicable if the entity taking the network trace is downstream of the target station (the station receiving the frames) and upstream of the source station (the station sending the frames).

The following methods can be used to determine if a station may not have received all frames intended for it. These methods investigate whether or not the station has experienced receiver congestion, which indicates that the station did not receive the frames.

- If the station supports the IEEE 802.5 MIB, a non-zero value for the dot5StatsReceiveCongestions object indicates that the station has experienced receiver congestion.
- If the 8239's RMON Ring Station Group is enabled, issue DISPLAY RMON RING_STATION_DATA HOST_ADDRESS several times, specifying the station's MAC address; verify whether the Congestion Errors counter is non-zero. To determine whether the RMON Ring Station Group is enabled, issue DISPLAY RMON GROUP_STATUS. To enable the Ring Station Group, issue ENABLE RMON RINGSTATION. This method can be used only if the station is inserted into the ring and participating in the Neighbor Notification process.
- REM can be used to indicate whether any station is sending out Soft Error Report MAC frames indicating receiver congestion. To use this approach, the 8239 Model 1 must be configured in these ways:
  - Surrogate Group Enabled – To see the current setting, issue DISPLAY TR_SURROGATE SURR_STATUS. To enable it, issue ENABLE TR_SURROGATE SURR_STATUS SURR_ADMIN.
  - REM Group Enabled – To see the current setting, issue DISPLAY TR_SURROGATE SURR_STATUS. To enable it, issue ENABLE TR_SURROGATE SURR_STATUS REM_ADMIN.
  - REM Traps flag Enabled – To see the current setting, issue DISPLAY TR_SURROGATE REM_STATUS. To enable it, issue ENABLE TR_SURROGATE REM_STATUS REM_TRAPS.
  - REM Ring Receiver Congestion Data Enabled – To see the current setting, issue DISPLAY TR_SURROGATE REM_STATUS. To enable it, issue ENABLE TR_SURROGATE REM_STATUS RING_RCVRCNGST_ERROR_DATA.[3]

[3] Enabling RING_RCVRCNGST_ERROR_DATA will result in a trap's being issued each time a station sends a Soft Error Report MAC frame with a non-zero value for the receiver congestion counter; the display of excessive traps may result. This flag should be enabled for specific circumstances only and not for general operational use.

Check the Neighbor Notification Process

The Neighbor Notification process, also known as the *ring poll process*, consists of the active monitor periodically broadcasting the Active Monitor Present (AMP) frame to all ring stations on its ring; all other stations subsequently send Standby Monitor Present (SMP) frames. The AMP and SMP frames from a station contain the address of its nearest active upstream neighbor (NAUN). The 8239 address-to-port mapping function and the 8239 RMON agent use these AMP and SMP frames to identify the stations that are active and their physical order. If the Neighbor Notification process does not complete successfully, there is a problem with the network. The following signs indicate that the Neighbor Notification process is not completing successfully:

- Stations cannot insert into the ring.
- 8239 address-to-port mapping data may not be available or accurate (verify using DISPLAY NETWORK_MAP).
- 8239 RMON Ring Station data may not be available or accurate (verify using DISPLAY RMON RINGSTATION_DATA).
- Active Monitor sends out a Report Neighbor Notification Incomplete (NNI) MAC frame. NNI conditions are not an object in any of the common industry standard MIBs (such as RMON or RFC-1231) or private MIBs (such as the IBM Token Ring Surrogate MIB or the 8239 MIB), so it is not easy to verify whether this condition is occurring. The simplest way to verify this condition is to obtain a network trace and check for the presence of NNI frames. If the 8239's RMON MAC Layer Statistics group is enabled, use an RMON manager to set up a packet capture and filter for all MAC frames or use an external network analyzer.

To determine whether the Neighbor Notification process is completing successfully, obtain a network trace and verify that the AMP and SMP frames are correct. To obtain the network trace, use one of these methods:

- If the 8239's RMON MAC Layer Statistics group is enabled (see "Check the RMON Group Status" on page 5-48), use an RMON manager to set up a packet capture and filter for all MAC frames.
- Use an external network analyzer

Some occurrences that can prevent the Neighbor Notification process from completing successfully are:

- Hard errors on the ring. See "Check for Hard Errors (Beaconing) on the Data Network" on page 5-31.
- Soft errors on the ring. See "Check for Soft Errors on the Data Network" on page 5-34.
- A problem with the station that prevents it from participating in the Neighbor Notification process.

Note that multiple ring polls can occur simultaneously. This event is normal when reconfiguration occurs, that is, when two segments are joined together. The situation should resolve itself automatically, but persistent soft errors on the ring can prevent the resolution of multiple ring polls.

Remove a Station

This section describes the methods available to remove a specific station from the data network.

If the station is locally attached to the 8239, disable the port using the DISABLE PORT terminal interface command, which causes the port to get wrapped from the network. No change is made to the station except that the station will be by itself on its own segment.

Note: If the station that needs to be removed from the network is the 8239 Model 1's Management Interface, the only way to remove it from the network is to administratively disable it by issuing SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE . You can use RMON or CRS to issue a Force Remove MAC frame to the Management Interface's MAC address, but the Management Interface will not accept the request and will return a negative response; this prevents another station from being able to control the Management Interface and disrupt connectivity to the 8239 stack.

The 8239 Model 1's RMON or CRS functions can be used to cause a station on the same segment as the Management Interface to remove itself from the ring. To use RMON to remove a station, the Ring Station Statistics group must be enabled; the only method of instructing the 8239 using RMON to issue a Force Remove MAC frame to a station is via SNMP. Either SNMP or the terminal interface can be used to cause the Model 1's Configuration Report Server (CRS) to issue a Force Remove MAC frame to a given station. From the terminal interface, issue SET TR_SURROGATE CRS_STATION REMOVE_STA. The following functions must be enabled:

Item to Configure	Terminal Interface Command to Display Current Setting	Terminal Interface Command to Enable the Item
Surrogate Function	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN SURR_STATUS
CRS Group	DISPLAY TR_SURROGATE SURR_STATUS	ENABLE TR_SURROGATE SURR_ADMIN CRS_STATUS

Verify the Physical Path Between Hubs

Each of the hubs must be part of the same control ring that is formed by the SI/SO connections in order to form a stack and provide device management capability for all of the hubs in the stack . Verify that the all the hubs are inserted into the control ring using "Check CI/CO Status" on page 5-42.

Verify that the Control Interface MAC is Inserted

In order to communicate with other hubs in the stack, the hub's control interface MAC must be inserted into the control ring. When the Control Ring Interface is inserted into the network, both of the following conditions must be true:

- The Control Ring Interface must be unwrapped. See"Check CI/CO Status" on page 5-42 .
- The Control Ring Interface's adapter must be opened onto the ring. The 8239 automatically tries to open onto the ring.

To verify that the hub's control ring interface is inserted into the ring, issue a DISPLAY STACK teminal interface command with two or more hubs connected. The results from this command should list all of the hubs in the stack. If one of the hubs is not listed, isolate that hub from the control ring by issuing WRAP CONTROL_IO BOTH ; use a locally attached terminal connected to that hub's EIA-232 interface. If the isolated hub is able to open its adapter successfully, then it should be a single station on the ring, as indicated by the Singles counter displayed when DISPLAY COUNTER CONTROL_RING is issued. If the Control Ring MAC interface was able to open, unwrap the CI/CO connections to put the hub back in the stack. After waiting at least one minute to allow the ring to reconfigure and connectivity to be established between the hubs, issue DISPLAY STACK again. If all of the hubs still do not appear in the list, there may be a problem with the control ring or the SI/SO cables that either prevents the Control Ring MAC interface from opening onto the ring or prevents connectivity between hubs. See "Check for Errors on the Control Ring." If the control ring and cables are OK, there may be a problem with the 8239 itself; contact your provider of service.

Check for Errors on the Control Ring

To determine the errors that may be present on the control ring, repetitively issue the DISPLAY COUNTER CONTROL_RING terminal interface command. This command can be executed only on the hub on which the command is issued. The counters displayed are the IEEE 802.5 counters. If any of the counters continue to increment, there are errors on the control ring. Depending upon their frequency, the errors may be sufficient to degrade performance of the control ring. The errors are either soft errors or hard errors.

If hard errors are occurring, the Hard Errors counter or the Transmit Beacons counter increments. If it is concluded that the 8239 is in the fault domain of the beaconing, then the Auto Removals counter is non-zero. The 8239 has a beacon recovery algorithm on the control ring to automatically detect and isolate faults that result in hard errors. If a fault is found off the Control In or Control Out connection, then that connection is wrapped to remove the fault. To determine whether part of the control ring has been wrapped due to beaconing, issue DISPLAY WRAP_POINTS. The CI/CO status will be BEACON WRAPPED if a beacon fault was detected from that connection. The 8239 will automatically unwrap the connection once the fault has been removed.

If soft errors are occurring, the Soft Errors counter and the appropriate counters that represent soft errors will increment. When soft errors are present on the control ring, there are no automatic mechanisms to isolate or remove the soft errors. If the soft error counters are incrementing on this hub and they are suspected of causing connectivity problems, use WRAP CONTROL_IO; start with the hub that is reporting the soft errors or the hub that is cabled to the Control In connection of the hub reporting the soft errors. After each wrap command is issued, wait at least one minute to allow the control ring to stabilize after reconfiguring itself; then issue a terminal command, such as DISPLAY STACK, that allows you to verify which hubs are in the control ring and whether they can communicate successfully to one another.

If connectivity between the hubs on the control ring is improved by wrapping out certain connections, check the Stack In/Stack Out cable for errors. If the cable is OK, gather the information described in "General Information about the 8239" on page 5-24; then, individually reset the suspect hubs, waiting to see if

communications improves once the hub that was reset becomes operational. If the problem persists, contact your provider of service.

If any of the CI/CO connections were wrapped, remember to issue UNWRAP CONTRO_IO to configure the connection for normal operation.

Check for a Fatal Error on the Hub

If the hub is not responding as you expect, follow these steps to determine if the hub is operational:

- Issue a terminal interface command, such as DISPLAY HUB, to check for a hub response. You may need to connect the terminal to the hub's EIA-232 interface to perform this step.
- Cause a station to insert into the ring or deinsert from the ring and verify that:
  - The station was properly inserted or deinserted
  - The port LED is correct after the change

If the hub does not appear to be responding as desired, gather the information described in "General Information about the 8239" on page 5-24 and then reset the hub. If the problem persists, contact your provider of service.

Check the RMON Group Status

To view the current settings of the RMON groups, issue the DISPLAY RMON GROUP_STATUS terminal interface command. To enable the RMON group, issue ENABLE RMON. The status and configuration of any RMON groups that are not listed on DISPLAY RMON GROUP_STATUS, especially the RMON 2 groups, can be accessed only via SNMP.

Clearing or Deleting an RMON Table

When an RMON table becomes full, new entries are not added. You must clear or delete the RMON table for the table to be automatically rebuilt based on current traffic data. You can clear RMON tables through SNMP or the terminal interface. RMON 2 tables can be cleared only using SNMP.

Depending on your network configuration and network traffic characteristics, you may need to periodically clear the RMON and RMON 2 tables. RMON events and alarms can be used to indicate, via SNMP, when a table is full. If the RMON Manager does not provide a user interface for checking the status of the table, you can use a MIB Browser.

To view the maximum number of entries for each RMON table, see "RMON Tables" on page 8-19.

Use the following methods to clear or delete the current contents of the RMON tables:

- Disable the RMON or RMON 2 group. You can disable RMON through SNMP or through the terminal interface, using the DISABLE RMON terminal interface command. You can disable RMON 2 only through SNMP.
- Clear the appropriate tables using CLEAR RMON.

  Note: This method applies to all RMON tables except for the tables under CLEAR RMON STATISTICS_DATA. CLEAR RMON STATISTICS_DATA only clears the statistics counters when they are displayed using the terminal interface, ***not*** through SNMP.

Chapter 6. Concentrator Functions

The functions that are described in this chapter are:

- Port Concepts
- Address-to-Port Mapping
- Port Security
- Ring In/Ring Out Concepts
- Stack Concepts
- Beacon Recovery

Unless otherwise noted, these functions are supported on both models of the 8239.

To configure or obtain status information related to the concentrator functions, use one of these methods:

- A terminal interface command using the EIA-232 interface
- A terminal interface command using a Telnet session to an 8239 Model 1 in the stack
- An SNMP request to the appropriate object in the IBM 8239 MIB (*8239 MIB*) issued to an 8239 Model 1 in the stack

Instructions for accessing information in the remainder of this chapter describe only access through the terminal interface command.

For a complete listing of commands referenced in this chapter, see the *8239 Command Reference*.

Port Concepts

Token-Ring workstations access an 8239 stack ring by being connected to an 8239 port. Each 8239 hub contains 16 RJ-45 ports. Cabling can be either unshielded twisted pair (UTP) or shielded twisted pair (STP). An optional port expansion card is available to increase the number of RJ-45 ports in the hub from 16 to 32. The port expansion card is inserted into a feature slot on the 8239 and is hot-pluggable. Refer to “16-Port Expansion Adapter” on page 3-1 for more information on installing or removing the port expansion card.

Port Configuration Options

When a Token-Ring station that generates phantom voltage is cabled to the 8239 port, ***no*** default value changes are necessary for that station to insert into the ring. If the device attached to the 8239 port does not provide phantom voltage, then that port needs to have 8228_mode enabled in order to insert into the ring. Some additional configuration options are also described in this section.

Port Administrative Mode

In order for a port to insert into the ring, the administrative mode for that port needs to be enabled. The default setting for the port administrative mode is enabled. To disable the port administrative mode, issue the DISABLE PORT terminal interface command. When the port is enabled, the port’s green status LED is initially off. When the port is disabled, the port’s green status LED is blinking.

8228 Mode

Normally, the 8239 checks for the presence of phantom insert voltage to determine when a station is ready to insert into the ring. Some devices such as the IBM 8228 (generically referred to as fanout devices) do not provide phantom voltage. To allow these types of devices to be inserted into the ring, the 8239 supports a port setting called *8228_mode*. When 8228_mode is enabled, the 8239 will not wait for phantom voltage to be present but will automatically proceed with the port insertion process. The default setting for 8228_mode is disabled. To enable 8228_mode, issue the ENABLE PORT_SETTING 8228_MODE terminal interface command.

Note: Enabling 8228_mode when the port is not connected to a valid device will cause network disruptions.

Speed Detect and Speed Threshold

The 8239 is able to verify that the station requesting to insert is running at the same speed as the ring. If the ring speeds of the station and the ring do not match, the 8239 does not allow the station to insert, preventing disruption to the ring. This ring speed verification is done only when the speed_detect port setting is enabled. The default value for speed_detect is enabled. To disable the port from automatically performing speed detection, issue the DISABLE PORT_SETTING SPEED_DETECT terminal interface command. Speed detection is configured on a per-port basis.

When speed_detect is enabled, the 8239 allows a station running at a different speed to continue to request insertion until it exceeds the speed-mismatch threshold value. The default value for the speed mismatch threshold is 8 and is associated with a given hub. To display or change the speed-mismatch threshold value, issue the DISPLAY HUB or SET HUB SPEED_THRESHOLD terminal interface commands, respectively.

The speed threshold is configured on a per-hub basis.

Beacon Threshold

When the 8239 detects that a port is the source of a beacon fault, that port is automatically wrapped. The 8239 has a beacon threshold value to prevent the same port from causing problems indefinitely on the network. The default value for the beacon threshold value is 8. To display or change the beacon threshold value, issue the DISPLAY HUB or SET HUB BEACON_THRESHOLD terminal interface commands, respectively.

Beacon threshold is configured on a per-hub basis.

Port Up/Down Traps

The 8239 can be configured to send a Port up/down trap whenever a port is inserted or deinserted. There are two types of configuration parameters associated with Port up/down traps:

- A parameter that is global for the entire hub: You display this parameter by issuing the DISPLAY TRAP_SETTINGS terminal interface command and looking at the value of Port Up Down. The default value is enabled. To change the value of the Port Up Down trap_setting, issue the ENABLE/DISABLE TRAP_SETTING PORT_UP_DOWN terminal interface command. When the port_up_down trap_setting is enabled, traps are sent when the port goes up or down.

- A parameter that is associated with a given port: You display this parameter by issuing the DISPLAY PORT terminal interface command and looking at the value of Traps. The default value is enabled. To change the value of the port's trap setting, issue the ENABLE/DISABLE PORT_SETTING TRAPS terminal interface command. When the port's trap setting is enabled, traps are sent when the port goes up or down provided that the global TRAP_SETTING PORT_UP_DOWN is also enabled. When the port's trap setting is disabled, traps are not sent when the port goes up or down, even if the global TRAP_SETTING PORT_UP_DOWN is enabled.

For more information about traps, refer to "Trap Processing" on page 7-12.

Port Groups

The 8239 lets you assign one or more ports to a group. You can then issue a single command to enable or disable a set of ports. The group can consist of any ports in the stack. It also can be pre-configured with ports that will eventually be part of the stack. A descriptive name is assigned to the group so that it can be referenced by name. Ports can be added or removed selectively from the group.

The default setting has no groups defined. To set up a group, issue the following terminal interface commands:

1. SET GROUP NAME to assign a name to a port group
2. SET GROUP PORT to assign ports to a port group

The following terminal interface commands are related to port groups:

- CLEAR GROUP NAME
- CLEAR GROUP PORT
- DISPLAY GROUP
- ENABLE/DISABLE GROUP
- SET GROUP NAME
- SET GROUP PORT

16-Port Expansion Adapter

No configuration changes are needed when the port expansion card is used. Ports on the 16-Port Expansion Adapter have the same characteristics as the base set of ports.

Inserting/Deinserting a Station

Before allowing a station to insert into the ring, the 8239 makes sure that the following conditions are met:

- The port's administrative mode is enabled
- Phantom voltage is present at the port or the port's 8228_mode setting is enabled
- The port's counters have not exceeded either the beacon threshold value or the speed-mismatch threshold value set for the hub
- The station connected to that port is running at the same ring speed as the hub

Some stations are unable to successfully insert into the ring when they are unable to receive the ring parameters from the Ring Parameter Server (RPS) on the ring, if present. In this state, the station's adapter is in receive congestion state and cannot complete its Open Adapter insertion process. To correct this problem, the 8239

supports a *purge on insert* process which, when enabled, causes the adapter to clear out its receive buffers so that it can receive the frame from RPS. The default value for “purge on insert” is enabled. To display the setting, use the DISPLAY HUB terminal interface command. To change the setting, issue the ENABLE/DISABLE PURGE_ON_INSERT terminal interface command.

Note: “Purge on insert” is not necessary and can be disabled whenever any of the following conditions exists:

- There is no RPS present on the ring.
- There is an RPS on the ring and the RPS sends the Request Initialization MAC Frame express-buffered. The 8239 Model 1 RPS operates in this way so that when the Model 1 RPS is active, “purge on insert” can be disabled.

Once a port is successfully inserted into the ring, the port status is changed to OK and the port’s green status LED is changed to on.

Port Operational Status and Port LEDs

To display the port status, issue the DISPLAY PORT terminal interface command. The values for the port status and the state of the port’s LEDs are as follows.

- **Port administrative mode is enabled**
  - And phantom voltage is present
    - Port status is OK when the port is successfully inserted. The green LED is on; the yellow LED is off.
    - Port status is BEACON WRAPPED when the port was detected to be the source of beaconing. The green LED is off; the yellow LED is on.
    - Port status is BCN THRES ERROR when the number of times the port had a beacon fault exceeded the beacon threshold value. The green LED is off; the yellow LED is blinking.
    - Port status is SPEED MISMATCH when the port tried to insert at the wrong speed. The green LED is off; the yellow LED is on.
    - Port status is SPD THRES ERROR when the number of times the port tried to insert at the wrong speed exceeded the speed mismatch threshold value. The green LED is off; the yellow LED is blinking.
    - Port status is SECURITY BREACH when a MAC address off of that port was not configured in the Secure Address Table (refer to “Port Security” on page 6-7 for details). The green LED is off; the yellow LED is blinking.

    Note: When the port status is BCN THRES ERROR, SPD THRES ERROR, or SECURITY BREACH, the port is considered to be permanently wrapped and cannot be inserted into the network again until it is administratively re-enabled by issuing the ENABLE PORT terminal interface command.
  - And phantom voltage is not present

    Port status is NO PHANTOM; the green LED is off and the yellow LED is off.
- **Port administrative mode is disabled**

The port's green LED is blinking; the yellow LED is off. The port status will be:

- PHANTOM when phantom voltage is present
- NO PHANTOM when phantom voltage is not detected

For more information about the port status LEDs, refer to "Port Status" on page 5-3.

Address-to-Port Mapping

To aid network administrators in managing their networks, the 8239 provides information that identifies which MAC addresses are connected to which ports on the 8239. This capability is called *address-to-port mapping* and is also referred to as *mapping*. No configuration options are needed for the 8239 to perform mapping; it is done automatically and the mapping information is available on request.

Stations that are directly attached to one of the 16 or 32 ports on an 8239, including fanout devices and MAC-less devices, are referred to as *local stations*. Stations attached to external devices can also be identified when an 8239 Model 1 is used; these stations are referred to as *external stations*.

Mapping identifies what MAC addresses or set of MAC addresses (if a fanout device is used) are assigned to a port. Mapping also determines if a MAC-less station is attached to an 8239 port.

Fanout Devices

A fanout device is a device to which multiple stations can be attached; the device itself is then attached to a single port on the 8239. The IBM 8226 and the IBM 8228 are examples of fanout devices.

Note the following considerations for the attachment of fanout devices to an 8239 port:

- If a fanout device has more than 8 stations attached to it, only the first 8 stations are identified with a hub and port assignment; all other stations on the fanout device are identified as "External" if information is being displayed using an 8239 Model 1 that has RMON ring station statistics group enabled.
- If no active stations are attached to the fanout device, the fanout device is recognized as a MAC-less device.
- A MAC-less device that is attached to the fanout device, as opposed to being attached to the 8239 port, will not be included in the mapping information.
- The ability to display fanout devices does ***not*** depend on whether or not 8228_mode is enabled for a port (refer to "Port Concepts" on page 6-1).
- If multiple fanout devices are attached to consecutive active ports and the last station on the first fanout device is moved to the first station on the next fanout device, the mapping facility will not be able to detect the change.
- If multiple fanout devices are attached to the same 8239, it is recommended that you have at least one active single station inserted between the fanout devices.

MAC-less Devices

A MAC-less device is a Token-Ring station that inserts into the ring but does not participate in the Neighbor Notification Process.

Note these considerations when MAC-less devices are attached to an 8239 port:

- To minimize the network disruption that occurs when identifying which port has a MAC-less device attached, it is recommended that you attach the MAC-less device at the last active port on the 8239. For example, if the 8239 has a 16-Port Expansion Adapter, attach the MAC-less device to port 32.
- To minimize network disruption, you should have at least one active station that participates in the Neighbor Notification Process attached to the hub to which an active MAC-less device is attached.
- MAC-less devices are represented as having a MAC address of “MAC-less Device” in the mapping information displayed.

Accessing the Address-to-Port Mapping Information

The mapping information that is gathered is referred to as the *network_map*. The network_map contains the MAC address, and the hub and port associated with that MAC address. Possible values for the port number are:

- A numeric value that represents the port number for a locally attached station
- “Management” when the MAC address is for an 8239 Model 1 in the stack
- “External” when either of the following conditions exists:
  - The MAC address is for a station that is part of the ring segment because it is attached via an 8239 RI/RO connection (see “Ring In/Ring Out Concepts (8239 Model 1 only)” on page 6-9).
  - The MAC address is connected to a fanout device that is locally attached to an 8239 port and there are already eight other stations listed for that port

  When a MAC address is listed as “External”, no hub number is listed.

“External” stations are included in the network_map only when an 8239 Model 1 is monitoring the ring with its RMON ring-station group enabled. The default value for the RMON ring-station group is enabled. Refer to “Configuring RMON” on page 4-7 for more details.

To obtain the address-to-port map information, use the DISPLAY NETWORK_MAP terminal interface command. This command allows various amounts of mapping information to be displayed:

- DISPLAY NETWORK_MAP ALL_STATIONS (8239 Model 1 command only) to list all locally attached stations within the segment containing the selected Model 1 and any external stations within that segment.
- DISPLAY NETWORK_MAP HUB to display only the stations locally attached to the specified hub. If this hub is an 8239 Model 1, Management Interface is also included if it is inserted on the ring.
- DISPLAY NETWORK_MAP LOCAL_STATIONS to display all stations locally attached to all the hubs on the stack data ring, including any Management Interfaces that are present. A maximum of eight stations per port will be displayed.

In addition to providing the MAC address-to-port mapping assignments, you can also find out the hub and port to which a specific MAC address is attached by using the DISPLAY NETWORK_MAP MAC_ADDRESS terminal interface command. The DISPLAY NETWORK_MAP PORT command allows you to find out what MAC addresses are associated with the specified port.

The mapping algorithm relies on the neighbor notification process. If there is network disruption such that the neighbor notification process does not complete successfully, then the network_map may not be up-to-date.

Note: When a ports_io wrap point is wrapped (for example, due to performing network problem isolation), the network_map may not be complete depending on which ports_io wrap points are wrapped and which network_map command is issued. Wrapping a ports_io wrap point is not recommended for normal operation.

When known external stations are not appearing in network_map (for example, in the DISPLAY NETWORK_MAP ALL_STATIONS command), the 8239's RMON ring station table may be full.To clear the RMON ring station table, issue the CLEAR RMON RINGSTATION_ALL terminal interface command to the IBM Model 1. Once the Token Ring Neighbor Notification Process completes successfully, subsequent displays of the network_map will include all currently active stations.

Port Security

The 8239 supports port security to allow the network to be secure against unwanted stations. The 8239 can be configured with MAC addresses that are allowed to insert at a given port. When an unauthorized station inserts into the ring (referred to as a *security intrusion* or *security breach*) and it is attached to an 8239 port, the 8239 will take the appropriate action based on what was configured.

To use port security, you must:

- Identify the MAC addresses that are authorized
- Configure the action on intrusion for that port
- Enable port security for the port

Identifying which MAC Addresses are Authorized

The list of MAC addresses that are authorized to insert at a given port is kept in a table called the Secure MAC Address Table. Each 8239 maintains its own Secure MAC Address Table. There can be a maximum of 16 MAC addresses per port in the Secure MAC Address Table. Port security is supported for fanout devices that are attached to the 8239.

Either of the following terminal interface commands can be used to specify which MAC addresses are put in the Secure MAC Address Table:

- SET SECURITY_PORT MAC_ADDRESS to assign individual MAC addresses
- SET SECURITY_PORT CAPTURE to copy all of the MAC addresses currently active on a given port into the Secure MAC Address Table

To display the MAC addresses in the Secure MAC Address Table, use the DISPLAY SECURITY PORT terminal interface command.

To remove a MAC address that is currently in the Secure MAC Address Table, use the CLEAR SECURITY_PORT terminal interface command.

Configuring the Action on Intrusion

When an unauthorized MAC address inserts at a port, the 8239 can be configured with any of the following actions:

- **disable and trap** to disable the port and send a trap
- **disable only** to disable the port
- **trap only** to send a trap
- **no action** to take no action

The default value for the action on intrusion is TRAP_ONLY. To change the action on intrusion, use the SET SECURITY_PORT ACTION_ON_INTRUSION terminal interface command.

When the port is disabled due to a security intrusion:

- A DISPLAY PORT command results in listing the port status as SECURITY BREACH
- The port's green status LED is off
- The port's yellow status LED is blinking

Once a port has been disabled due to a security intrusion, the port must be re-enabled before it can be inserted into the stack data ring again. The command to re-enable the port is ENABLE PORT.

When the 8239 is configured to send a trap on a security intrusion, the trap can be displayed on the terminal interface and it can be sent to an SNMP manager if a valid entry is in the trap community table for IBM 8239 traps. Refer to "Trap Processing" on page 7-12 for more information.

To display what security intrusions have occurred, use the DISPLAY SECURITY INTRUDER_LIST terminal interface command. The 20 most recent intrusions for the entire stack are displayed. An intruder will only be listed if the intrusions occurred when the hub is operational and part of the stack.

To clear all of the entries in the security intruder list, use the CLEAR SECURITY INTRUDER_LIST terminal interface command.

Enabling Port Security

In order for the 8239 to perform port security, port security must be enabled for each port desired. The default setting disables port security. To enable port security, use the ENABLE SECURITY_PORT terminal interface command.

Note: Port security should be enabled ***after*** the authorized MAC addresses are configured for the port so that premature actions on intrusions can be avoided.

Ring In/Ring Out Concepts (8239 Model 1 only)

The 8239 Model 1 contains a Ring-In/Ring-Out (RI/RO) slot that can be used to insert either an RJ-45 RI/RO Module or an Optical Fiber RI/RO Module. The 8239 RI/RO Module allows the 8239 stack to be connected to another 8239 stack or to other compatible hubs or concentrators. The RI/RO Module allows expansion of the network to include multiple devices that are a part of the same physical network.

The 8239 RI/RO Modules are not hot-pluggable. For information on installing and cabling a RI/RO Module or removing a RI/RO Module, refer to “RI/RO Module” on page 3-2.

RI/RO cables should be installed and connected at both ends before enabling (unwrapping) these interfaces. Any of these interfaces that are not going to be used should be administratively disabled (wrapped).

In a stack consisting of more than one 8239 Model 1, use caution when implementing a network with more than one RI/RO interface per stack. Multiple RI/RO connections between two ring segments or between two 8239 Model 1s in the same stack can cause undesirable results, such as a division of the ring into two independent segments.

The 8239 RI/RO ports emulate the IEEE 802.5 Dual Ring Recovery process to ensure there is high availability and reliability between the 8239 and any compatible devices connected to the 8239. The Dual Ring Recovery protocol ensures that there is an active, functional ring prior to unwrapping the RI/RO connection. If a fault occurs off the RI/RO connection, there is a known protocol to detect and correct the fault, where possible, and resume communications as quickly as possible.

RI/RO Configuration Options

There are two RI/RO configuration options:

- Administrative mode
- Up/down traps

RI/RO Administrative Mode

An administrative mode associated with each RI/RO indicates whether or not the RI/RO connection should be allowed to unwrap onto the ring if conditions are correct to do so. The default value for the RI/RO administrative mode is disabled. To enable the RI/RO administrative mode, issue either of the following terminal interface commands:

- ENABLE RING_IO
- UNWRAP RING_IO

Both of the above commands are equivalent. Two different commands are provided for the same function for flexibility.

When RI/RO is administratively enabled, the RI/RO’s green status LED initially is off and its status is WRAPPED. When RI/RO is administratively disabled, the RI/RO’s green status LED is blinking and its status is WRAPPED. To display RI/RO status, use the DISPLAY RING_IO terminal interface command.

RI/RO Up/Down Traps

The 8239 can be configured to send a RI/RO Status Up Down trap whenever the status of the RI/RO changes. This parameter is displayed by issuing the DISPLAY TRAP_SETTINGS terminal interface command and looking at the value of "Ring IO Status Up Down". The default value is ENABLED. To change the value of the Ring IO Status Up Down trap_setting, issue the ENABLE/DISABLE TRAP_SETTING RING_IO_STATUS_UP_DOWN terminal interface command.

For more information about traps, refer to “Trap Processing” on page 7-12.

Unwrapping the RI/RO onto the Stack Data Ring

After RI/RO is administratively enabled and is successfully connected to the external device, the RI/RO status is changed to UNWRAPPED and the RI/RO’s green status LED is changed to on.

A RI/RO Status trap may be generated to reflect the new RI/RO status.

RI/RO Operational Status and RI/RO LEDs

The possible values for the RI/RO Status and the associated LEDs are:

- RI/RO administrative mode is ENABLED
  - The RI/RO status is WRAPPED when the RI/RO cannot be successfully connected to an external device. The green LED is blinking and the yellow LED is off.
  - The RI/RO status is UNWRAPPED when the RI/RO is successfully connected to an external device. The green LED is on and the yellow LED is off.
  - RI/RO status is BEACON WRAPPED when the beacon fault is detected to be off the RI/RO connection. The green LED is off and the yellow LED is on.
- RI/RO administrative mode is DISABLED
  - RI/RO status is WRAPPED. The green LED is blinking and the yellow LED is off.

To display the RI/RO’s administrative mode and operational status, issue the DISPLAY RING_IO terminal interface command.

For information on the meaning of the RI/RO status LEDs, refer to“RI/RO Status” on page 5-6 .

Stack Concepts

Individual 8239 units can be connected to form a *stack*. Each 8239 contains a Stack In (SI) and Stack Out (SO) port that allows a customer to connect up to eight 8239s via standard Category 5 UTP cabling, providing a total of 256 ports in a single stack when port expansion cards are used. Any combination of 8239 Model 1s and 8239 Model 2s can be used within a stack. Refer to “Cabling a Stack” on page 2-5 and “Cable Types and Distances” on page 1-4 for details about cabling the stack and the types of cable that can be used, respectively.

Install and connect SI/SO cables at both ends before enabling (unwrapping) these interfaces. Administratively disable (wrap) any of these interfaces that are not going to be used.

The stack cables provide the medium for the control ring and stack data ring within the 8239 stack. The control ring is used for internal communications between 8239s in the stack. The stack data ring (also referred to as just the *stack ring*) carries user data traffic and specifically refers to the ring that forms when multiple 8239s are connected via their SI and SO ports.

Stack In contains the following elements:

- Control In (CI) for stack communications between 8239s
- Data In (DI) for the stack data ring

Stack Out contains the following elements:

- Control Out (CO) for stack communications between 8239s
- Data Out (DO) for the stack data ring

SI/SO Configuration Options

CI/CO and DI/DO are unwrapped under normal conditions so that stack communications can occur between 8239s in the stack and all user traffic can flow across the stack data ring. The default value for CI/CO and for DI/DO is UNWRAPPED, which is the setting required for normal operation. These connections are automatically unwrapped onto the control ring or data ring provided that the ring has normal operational status.

Commands are available to wrap or unwrap CI/CO administratively, but these commands are usually reserved for problem isolation and are not used for normal operation. The wrap commands are:

Note: Issuing the wrap commands can affect connectivity, so use the following terminal interface commands with extreme care.

- WRAP/UNWRAP CONTROL_IO for affecting stack connectivity
- WRAP/UNWRAP DATA_IO for affecting user traffic connectivity and segmentation

The ability to change the status of CI/CO is not available via SNMP.

To display the current wrap settings, issue the DISPLAY WRAP_POINTS terminal interface command.

CI/CO and DI/DO Up/Down Traps

The 8239 can be configured to send a CI/CO and DI/DO up/down trap whenever the status of the CI/CO and DI/DO changes. To display this parameter, issue the DISPLAY TRAP_SETTINGS terminal interface command and look at the values of Control IO Status Up Down and Data IO Status Up Down. The default value for both items is ENABLED.

To change the value of the Control_IO Up Down trap_setting and the Data_IO Up Down trap setting, issue the ENABLE/DISABLE TRAP_SETTING CONTROL_IO_STATUS_UP_DOWN and the ENABLE/DISABLE TRAP_SETTING DATA_IO_STATUS_UP_DOWN terminal interface commands, respectively.

For more information about traps, refer to “Trap Processing” on page 7-12.

SI/SO LEDs

There are three LEDs on each SI/SO connector: a green LED, a yellow LED, and another green LED.

The leftmost green LED indicates the wrap status for DI/DO, the stack data ring. The rightmost green LED indicates wrap status for CI/CO, the stack control ring. Green LED on indicates a status of unwrapped. Green LED blinking indicates a status of administratively wrapped. Green LED off means that the status is wrapped.

Yellow LED on means that there is a fault. The fault is associated with the connection that has green LED off.

For more information on what the Stack In/Stack Out status LEDs mean, refer to“Stack In/Stack Out Status” on page 5-7.

Beacon Recovery

To help improve network performance and network availability, the 8239 performs automatic beacon recovery when hard-error faults occur. The 8239 provides hardware-assisted beacon recovery technology to immediately detect when hard-error faults are present on the ring. The source of the fault is isolated by the 8239 to minimize the impact on the rest of the network. Once a hard error has been detected on the ring (that is, a station sends a beacon frame), single faults usually can be isolated in less than 1 second. Multiple faults take longer to isolate.

Faults can be found by the 8239 beacon recovery algorithm in the following areas:

- Data In/Data Out connection
- Port connection
- Management Interface (8239 Model 1only)
- Ring In/Ring Out connection (8239 Model 1 only)
- Within the 8239

The following sections describe these fault areas and the actions that are taken when the fault is removed.

Data In/Data Out Connection

When the beacon fault is found to originate from the Data In or the Data Out connection on the 8239, the 8239:

- Wraps the faulty DI/DO from the stack ring.
- Sends a DI/DO status trap to indicate the current state of the DI and DO. The faulty connection has a status of WRAPPED. Refer to “Trap Processing” on page 7-12 for details about sending the trap.
- Sets the status of the DI/DO to BEACON WRAPPED. You can display the DI/DO status by issuing the DISPLAY WRAP_POINTS terminal interface command. The DI/DO status will also be displayed on the LCD of any Model 1s in the stack. Refer to “Operational Codes” on page 5-15 for more information.

- Sets the faulty DI/DO's yellow status LED to on and sets the faulty DI/DO's green status LED off.

When the DI/DO on an 8239 is wrapped from the stack data ring, everything on that 8239 is isolated from the stack data ring, including ports, the Management Interface (Model 1 only), and any RI/RO connections (Model 1 only).

Once the DI/DO has been wrapped, the 8239 keeps automatically testing the DI/DO connection and then unwraps the DI/DO connection when it determines that the stack data ring has a normal operational status.

Port Connection

When the beacon fault is determined to originate from one of the ports on the 8239, the 8239:

- Isolates the port from the stack ring
- Sends a Port Down trap to indicate what port has been beacon-wrapped. Refer to "Trap Processing" on page 7-12 for details about sending the trap.
- Sets the status of the port to BEACON WRAPPED and increments the counter that indicates the number of times this port has been beacon-wrapped. The port status and beacon counter value can be displayed by issuing the DISPLAY PORT terminal interface command.
- Sets the port's yellow status LED to on and sets the port's green status LED off.

Once a port is beacon-wrapped, the 8239 will automatically unwrap the port when there is a recurrence of phantom at that port, as long as the port has not exceeded the beacon threshold. Refer to "Beacon Threshold" on page 6-2 for more information about the beacon threshold. When the number of times a port has been beacon-wrapped exceeds the configured threshold value, the port is considered to be permanently beacon-wrapped and the port status is set to BCN_THRES_ERROR. In this state, the port's yellow status LED blinks.

When a device that does not generate phantom voltage is attached to the port (refer to "Port Concepts" on page 6-1) or when a port has been beacon-wrapped due to exceeding the beacon threshold, manual intervention is required. After the fault has been corrected, you must re-enable the port by issuing the ENABLE PORT terminal interface command. This command sets the beacon counter for that port to zero.

Management Interface (8239 Model 1 only)

When the beacon fault is determined to originate with the Management Interface, the 8239 Model 1:

- Isolates the Management Interface from the stack ring.
- Indicates in the management_interface_status portion of the LCD that the Management Interface was beacon-wrapped. Refer to "Operational Codes" on page 5-15 for more information.
- Sets the adapter status of the Management Interface to BEACON WRAPPED and increments the counter that indicates the number of times the Management Interface has been beacon-wrapped. The Management Interface adapter status

and beacon counter value can be displayed by issuing the DISPLAY MANAGEMENT_INTERFACE terminal interface command.

Once the Management Interface is beacon-wrapped, the 8239 will automatically re-insert the Management Interface into the stack ring after the Management Interface verifies that its transmit and receive paths are OK. The Management Interface uses the beacon threshold value that is configured for the hub in the same way that the ports do. The default value for the beacon threshold value is 8. To display or change the beacon threshold value, issue the DISPLAY HUB or SET HUB BEACON_THRESHOLD terminal interface commands, respectively. When the number of times the Management Interface has been beacon wrapped exceeds the configured threshold value, the Management Interface is considered to be permanently beacon wrapped and the Adapter Status is set to BCN_THRES_ERROR. Once the Management Interface is in the permanently beacon wrapped state, an administrator must re-enable the Management Interface's administrative_mode to re-insert the Management Interface into the stack ring; to re-insert the Management Interface, issue the SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE DISABLE terminal interface command, followed by SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE ENABLE.

Ring In/Ring Out Connection (8239 Model 1 only)

When the beacon fault is determined to originate from the Ring In and/or Ring Out connection on the 8239, the 8239:

- Wraps the faulty RI/RO
- Sends a RI/RO status trap to indicate the current state of the RI and RO. The faulty connection has a status of WRAPPED. Refer to "Trap Processing" on page 7-12 for details about sending the trap.
- Sets the status of the RI/RO to BEACON WRAPPED. The RI/RO status can be displayed by issuing the DISPLAY WRAP_POINTS or DISPLAY RING_IO terminal interface commands. The RI/RO status will also be displayed on the LCD of any Model 1s in the stack. Refer to "Operational Codes" on page 5-15 for more information.
- Sets the faulty RI/RO's yellow status LED to on and turns the faulty RI/RO's green status LED off.

Once the RI/RO has been wrapped, the 8239 automatically keeps testing the RI/RO connection and then unwraps the RI/RO connection when it determines that there is a fault-free connection to the external device.

Within the 8239

The 8239 can determine if the beaconing fault is within the 8239. Such a fault can occur if there is an 8239 failure.

In this case, the 8239 automatically resets itself. Any unsaved configuration changes are lost. After the reset, the 8239 will not be operational if it failed its diagnostics.

Segmentation

This section provides guidelines for and examples of segmentation.

Rules for Segmentation

Note: The term *stack ring* is used throughout this section. The stack ring is the token-ring data path that runs throughout all the stack units via the Stack In /Stack Out cables. It is analogous to a backplane ring in a modular hub.

Follow these guidelines when creating segments:

- Every unit in the stack must be assigned to a segment. The factory default is that all units are assigned to the same segment.
- Segments may consist of one or more stack units using any combination of Model 1s or Model 2s. A single stack may consist of 1 to 8 data segments.
- Stack units in the same segment must be adjacent to each other in ring order; that is, Stack_Out of the first unit in the segment must be cabled to Stack_In of the second, and so on.
- When the Management Interface in a Model 1 is administratively enabled (unwrapped), it will be on the same segment as the ports on that Model 1.
- If the Ring In/Ring Out module is installed in a Model 1, the external stations are on the same segment as the ports on that Model 1.
- Make sure that in-band connectivity is maintained when the stack is segmented. For example, if the Network Management Station is attached to a switch that is also connected to one of the ports on the stack and that port ends up being on a different segment than the Management Interface, then you will lose in-band connectivity to the stack.
- The WRAP/UNWRAP DATA_IO commands are used to create segments.

  To create a single segment in a stack, all DI and DO connections on all 8239s must be unwrapped

  To create 2 or more segments in a stack when starting from a single segment stack:

  – Data In of the first unit in the segment must be wrapped

  – Data Out of the last unit in the segment must be wrapped

  To modify an existing multi-segmented stack, issue the appropriate wrap commands to cause:

  – Data In of the first unit in the segment to be wrapped

  – Data Out of the last unit in the segment to be wrapped

  – Both Data In and Data Out of all intermediate units (2 to *n*-1) in the segment to be unwrapped, where *n* is the number of units in the segment.
- Multiple segments are created in a stack by using the backup path of the data ring. In a single segment stack, the backup path is not normally used unless there is a fault in the stack portion of the ring. If a hard error occurs on a stack connection of the data ring (for example, in the stack cable as opposed to a port fault), the fault will be automatically detected and isolated. In the case of a single segmented stack, a fault on the stack connection will be wrapped and

the backup path is available for maintaining the data path across the segment. In the case of a multi-segmented stack, the backup path of the stack ring is no longer available for bypassing defective cables or stack units. In this case, when DI or DO is wrapped to isolate a fault, disjoint segments are formed until the fault is repaired.

- In order to monitor a segment, there must be a Model 1 on that segment with its Management Interface enabled.

Follow these guidelines when changing a segmentation configuration:

- If you are using in-band connectivity to your stack, be aware that connectivity can be lost when issuing WRAP DATA_IO commands to create your segments. It is recommended that you issue WRAP commands using out-of-band connectivity, that is, using the EIA-232 interface.
- Be aware that some attached stations may lose connectivity to servers, routers, and so on when WRAP commands are issued. After making segmentation changes, test connectivity to key stations to make sure you have not mistakenly lost connectivity.
- When you are monitoring a segment with a Model 1 and that segment changes, statistics collected by the Model 1 are not automatically cleared. The Model 1 will retain statistics related to the old segment, adding network management information for the new segment. For example, if a Model 1 was on a segment with 100 users and then the segment was changed, keeping 20 of its former users and adding 150, the Model 1 will collect data for the 170 current users and will retain information in its tables associated with the 80 former users. You should clear the network management statistics after making segment changes so that all data reported by the Model 1 is applicable to the current segment.

  If you are using in-band connectivity, clear the statistics by disabling and then enabling the network management functions:

  – Disable and enable all RMON groups (ENABLE/DISABLE RMON)
  – Disable and enable surrogate functions (ENABLE/DISABLE TR_SURROGATE SURR_STATUS)
  – Disable and then enable collecting of statistics for the 802.5 group (SET MANAGEMENT_INTERFACE 802.5_GROUP)
  – Reset the MIB II counters (CLEAR COUNTER)

    Note: This command only resets the counters when they are displayed using the terminal interface; it has no effect on the values of the counters obtained through SNMP.

  If you are using out-of-band connectivity, disable and then enable the Management Interface's administrative mode (SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE). Do not use this command if you are using in-band connectivity; connectivity will be lost when the Management Interface is disabled.

Segmentation Examples

After initial installation of a stack, all units are attached to the stack ring and create a single ring (which may be a part of an external ring if the RI/RO Module is installed and unwrapped). Use the WRAP commands to create multiple segments.

This section contains examples that illustrate the use of the WRAP commands to create various segment configurations. Figure 6-1 on page 6-18 through Figure 6-6 on page 6-28 show a stack consisting of one Model 1 and five Model 2 units. Figure 6-7 on page 6-30 and Figure 6-8 on page 6-32 show a stack of six units with three Model 1s and three Model 2s. For these examples:

- Assume that the stack started out in a normal initialized state with all units attached to the stack ring
- The control ring is not shown

Use Figure B-1 on page B-1, which identifies the wrap points for the Model 1 and Model 2, for general reference.

Single Segment

Figure 6-1 on page 6-18 shows a stack of six units, with a single Model 1, in the initial state. Note that all units are attached to the stack ring creating a single segment.

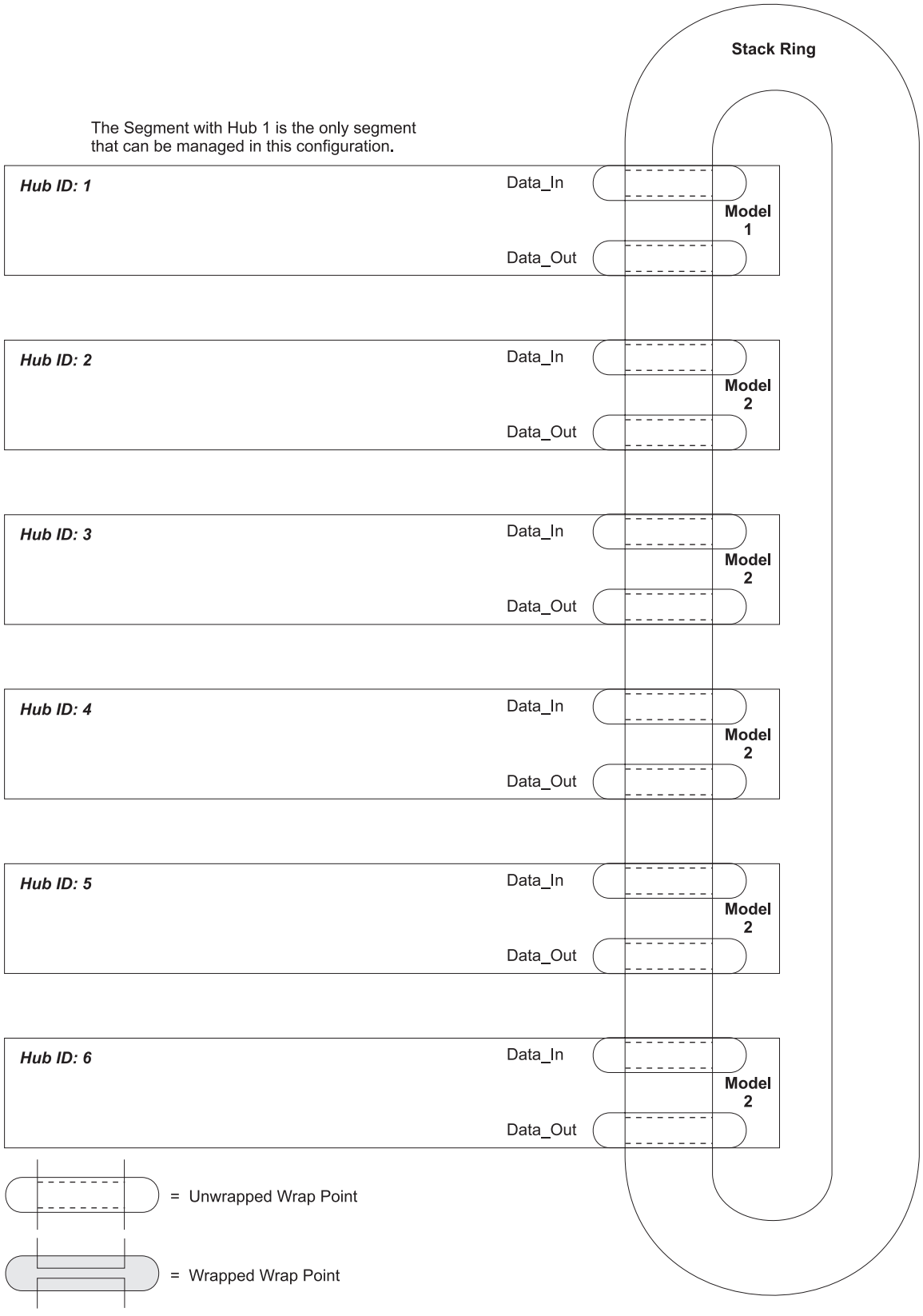

Figure 6-1. Single Segment with Six Units

Six Segments, Each with a Single Unit

To create 6 segments each with a single unit:

```
>>  wrap data_io both 1
>>  wrap data_io both 2
>>  wrap data_io both 3
>>  wrap data_io both 4
>>  wrap data_io both 5
>>  wrap data_io both 6
```

The resulting stack configuration is shown in Figure 6-2 on page 6-20.

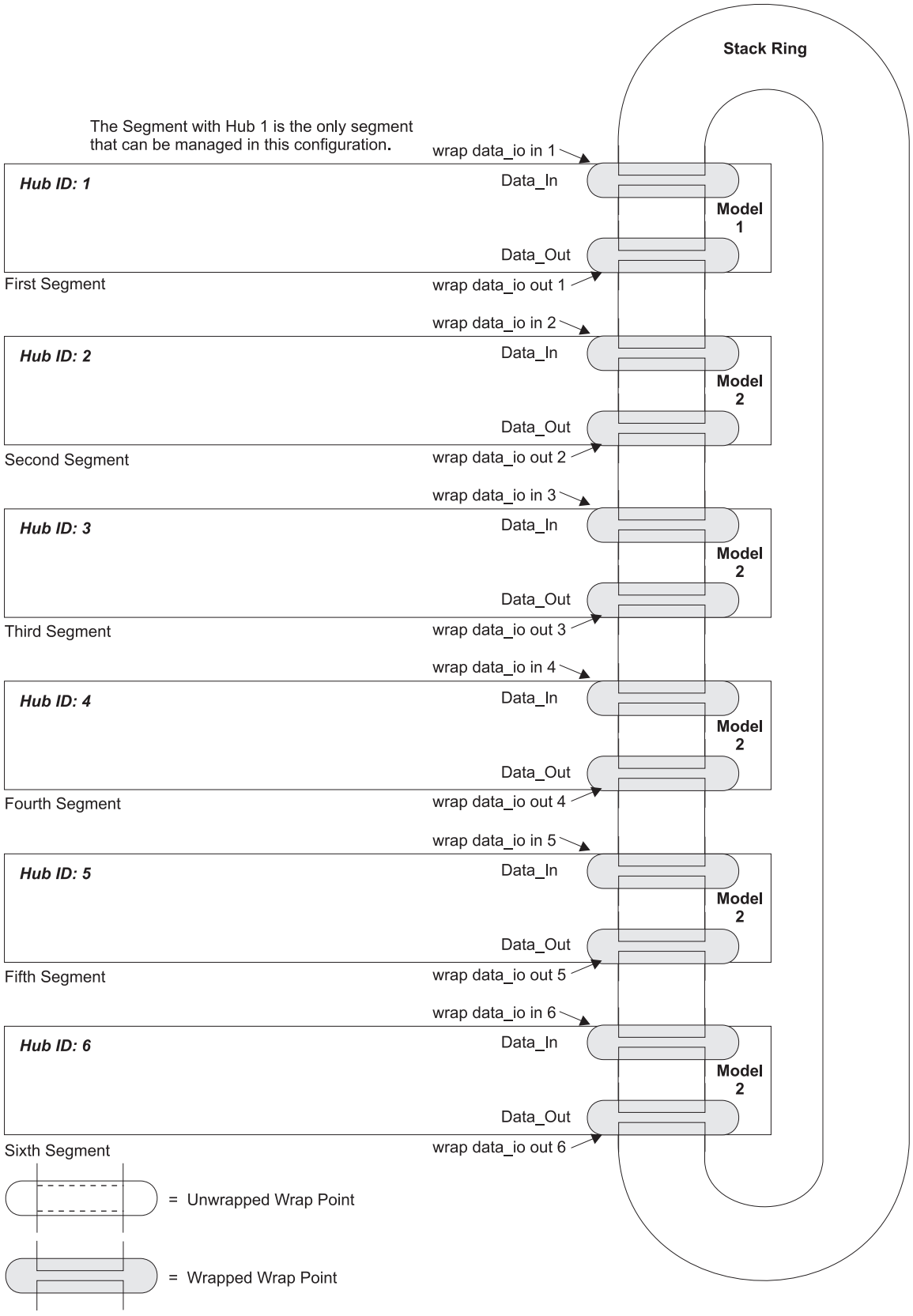

Figure 6-2. Six Units with Six Segments

Two Segments with One Unit Each and Two Segments with Two Units Each

To create four segments – two segments with one unit each and two segments with two units each – from the default configuration in Figure 6-1 on page 6-18, use these commands.

```
>>  wrap data_io in 1
>>  wrap data_io out 2
>>  wrap data_io both 3
>>  wrap data_io in 4
>>  wrap data_io out 5
>>  wrap data_io both 6
```

Figure 6-3 on page 6-22 shows the configuration of the stack after this command is executed.

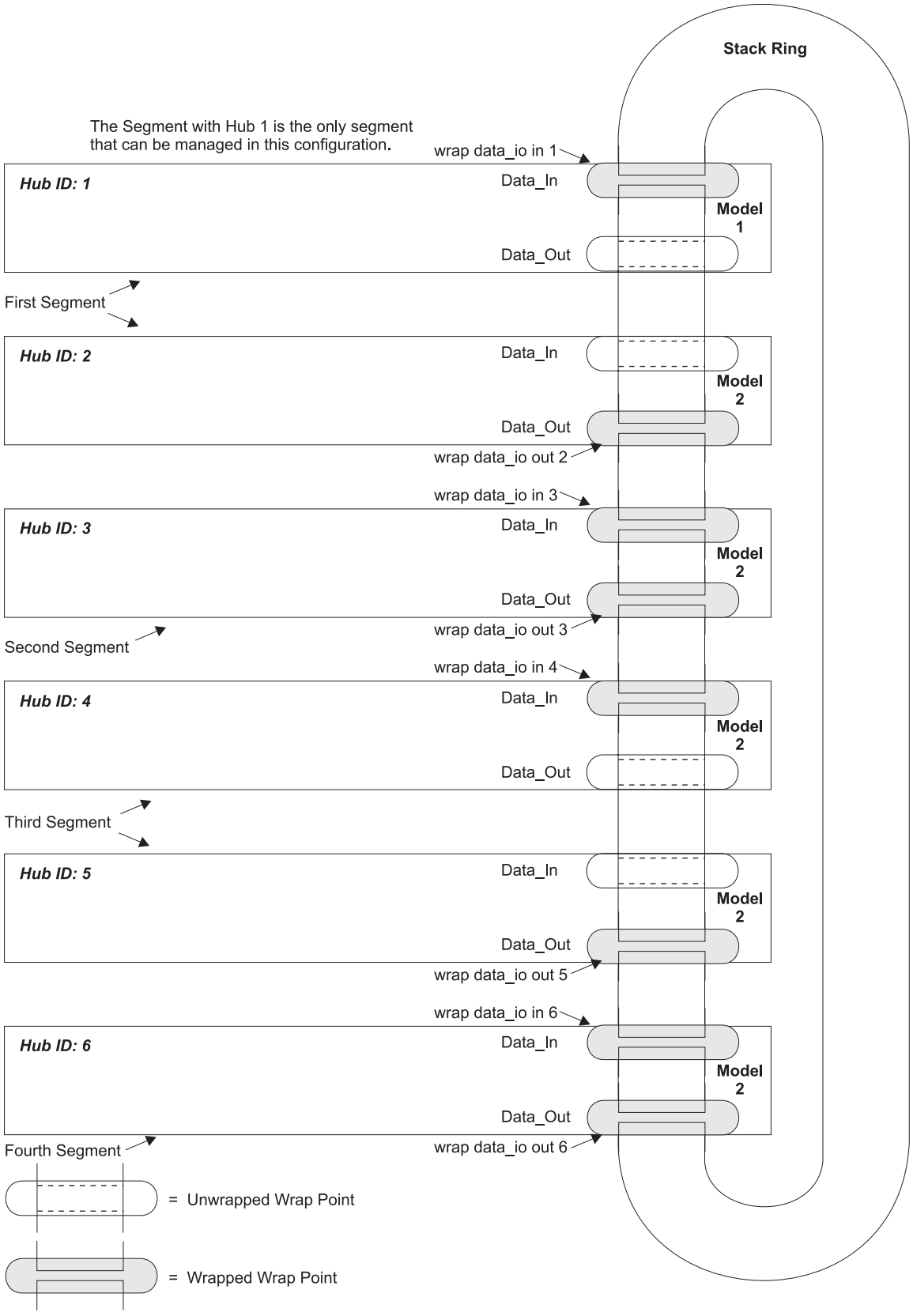

Figure 6-3. Two Segments

Two Segments with Three Units Each

To create two segments with three units each from the default configuration in Figure 6-1 on page 6-18, use these commands.

```
>>  wrap data_io in 1
>>  wrap data_io out 3
>>  wrap data_io in 4
>>  wrap data_io out 6
```

Figure 6-4 on page 6-24 shows this configuration.

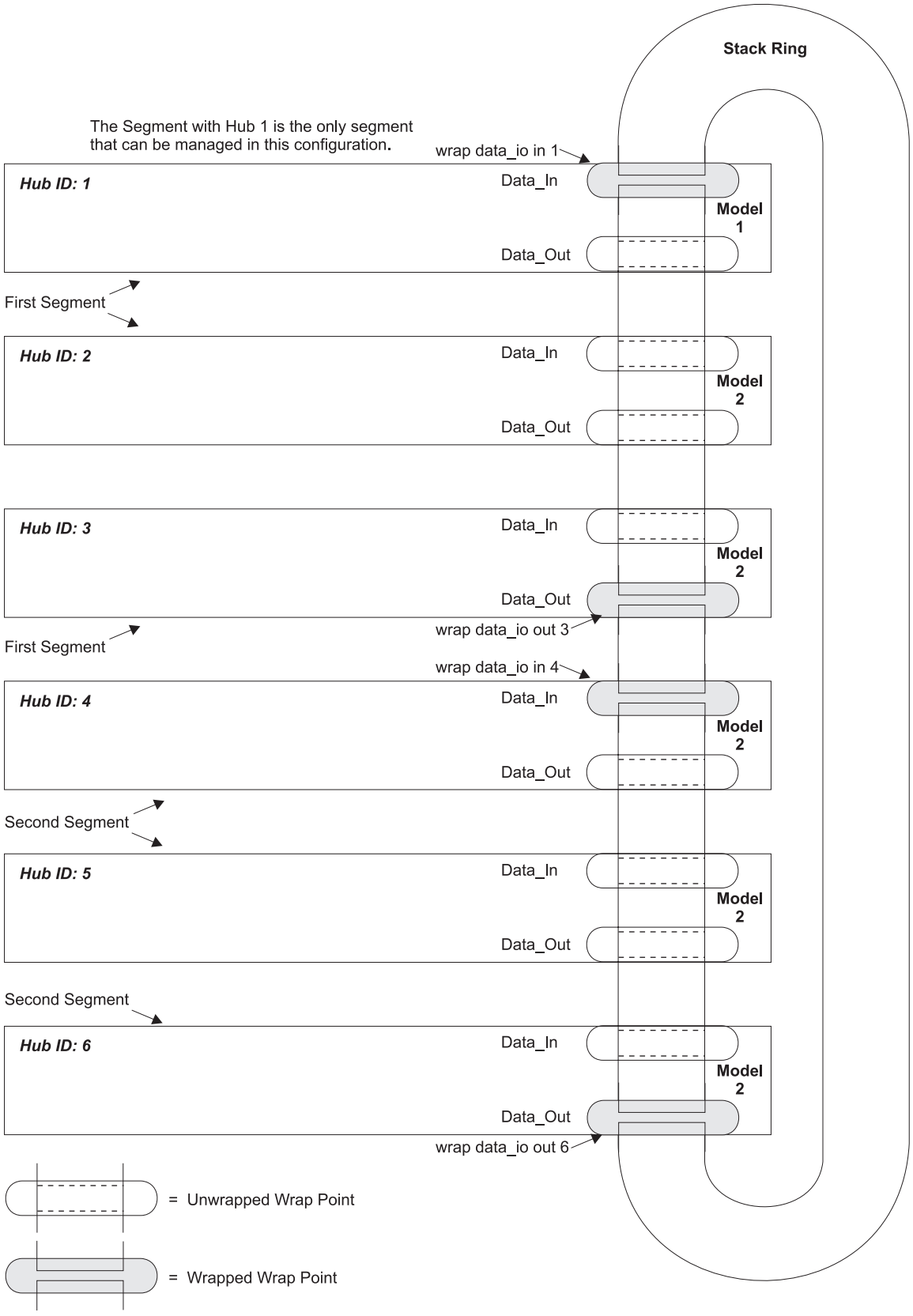

Figure 6-4. Two Segments of Three Units Each

Moving a Unit from One Segment to Another

Figure 6-5 on page 6-26 shows three segments:

- Hub 1 is a single-unit segment
- Hubs 2 and 3 make up the second segment
- Hubs 4, 5, and 6 make up the third segment

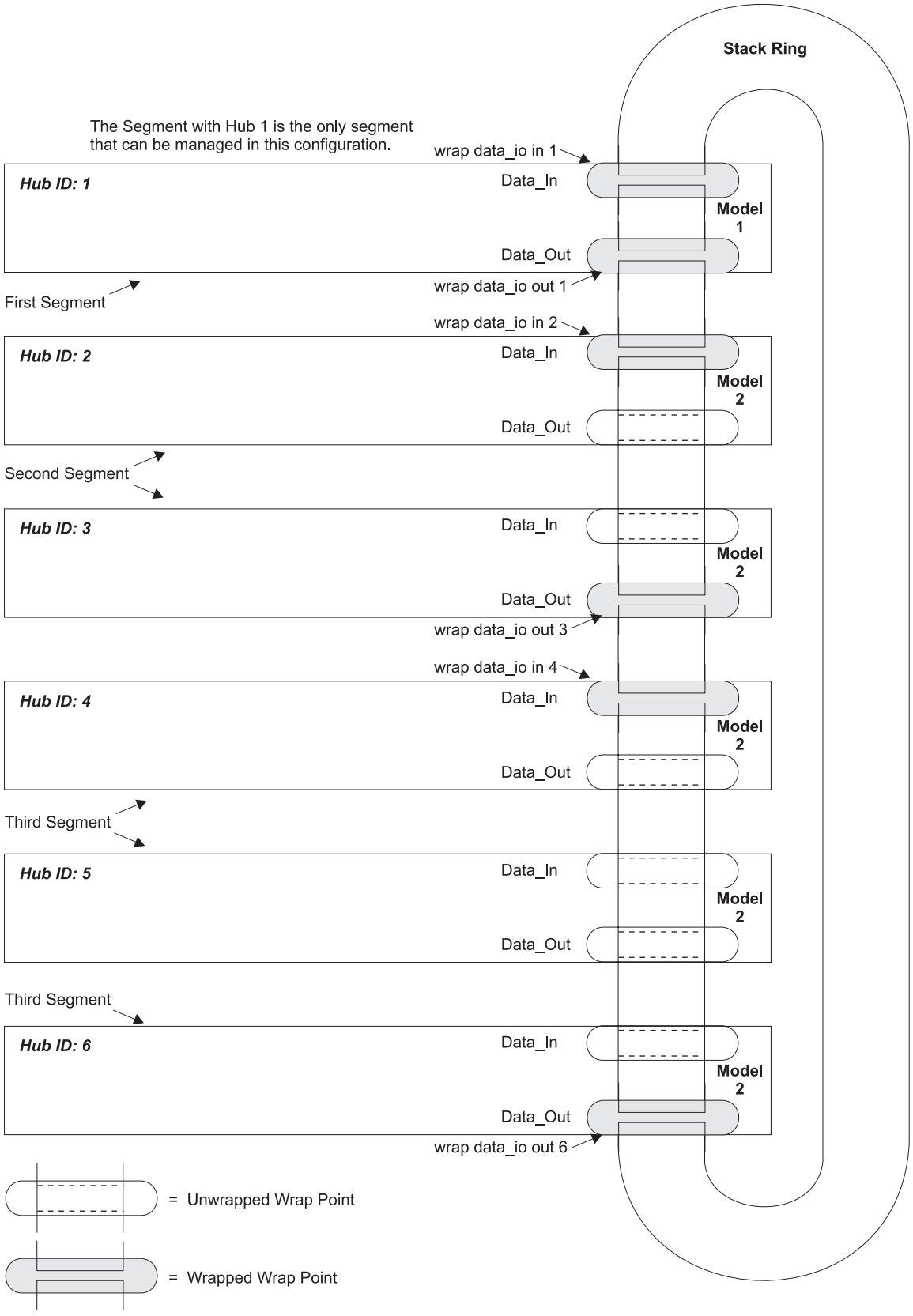

Figure 6-5. Six Units with Three Segments

To move hub 4 to the second segment, use the following commands:

1. Since hub 4 will now be the last unit in the segment, its Data Out should be wrapped

   ```
   >>  wrap data_io out 4
   ```

2. Since hub 5 will be the first unit in the third segment, its Data In should be wrapped

   ```
   >>  wrap data_io in 5
   ```

3. Data Out of hub 3 and Data In of hub 4 must be unwrapped to add hub 4 to segment 2

   ```
   >>  unwrap data_io out 3
   >>  unwrap data_io in 4
   ```

Figure 6-6 on page 6-28 shows the new configuration.

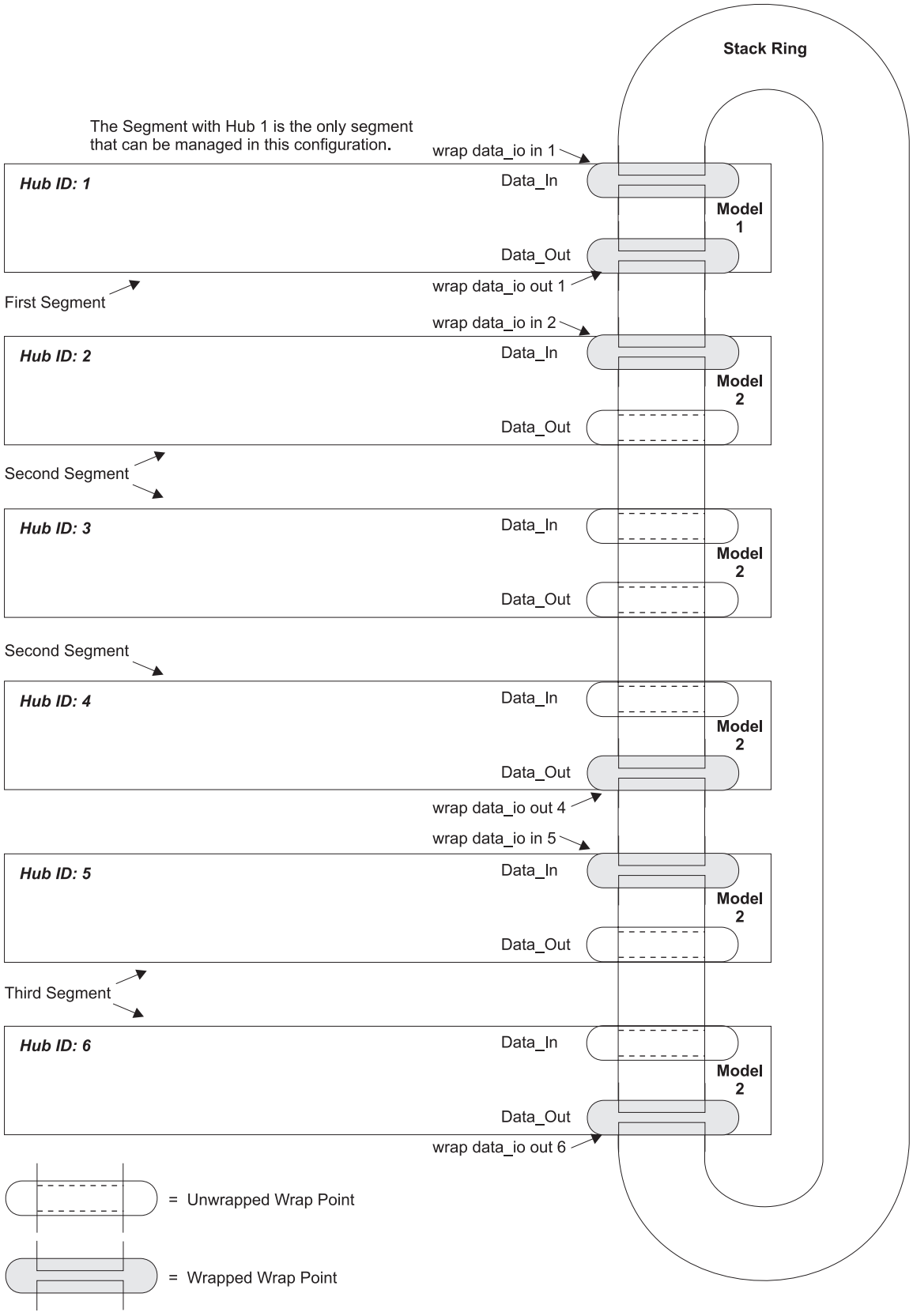

Figure 6-6. Six Units with Three Segments

Configuring Stacks with Multiple Model 1s

If you want concurrent full network management on all segments within a stack, a Model 1 for each segment is required. Figure 6-7 on page 6-30 shows a stack of six units – three Model 1s and three Model 2s – in the default configuration with all units in a single segment.

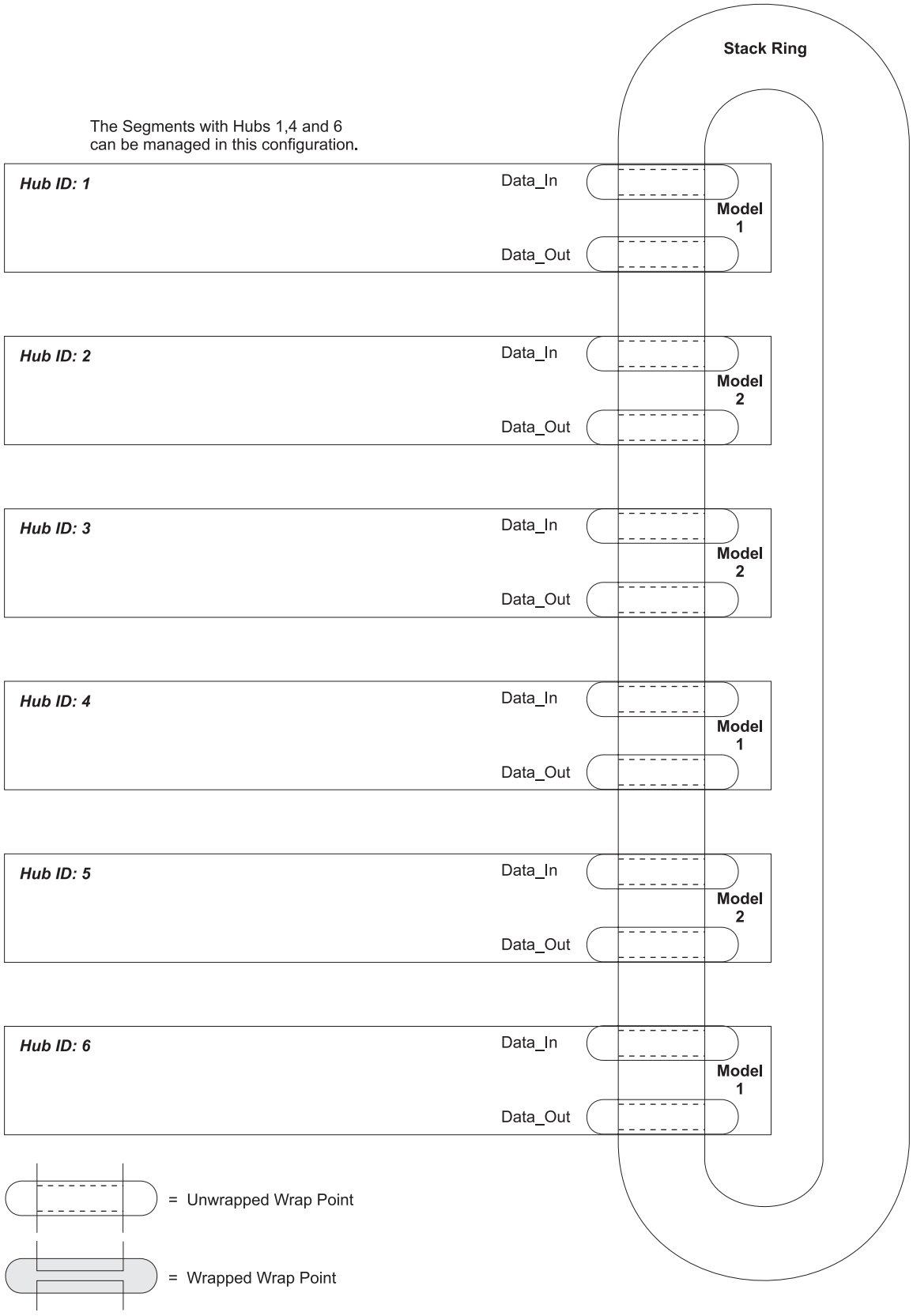

Figure 6-7. Six Units with One Segment

The stack can be configured into three fully managed segments. Figure 6-8 on page 6-32 shows such a configuration after the following commands are executed.

```
>>  wrap data_io in 1
>>  wrap data_io out 2
>>  wrap data_io in 3
>>  wrap data_io out 5
>>  wrap data_io both 6
```

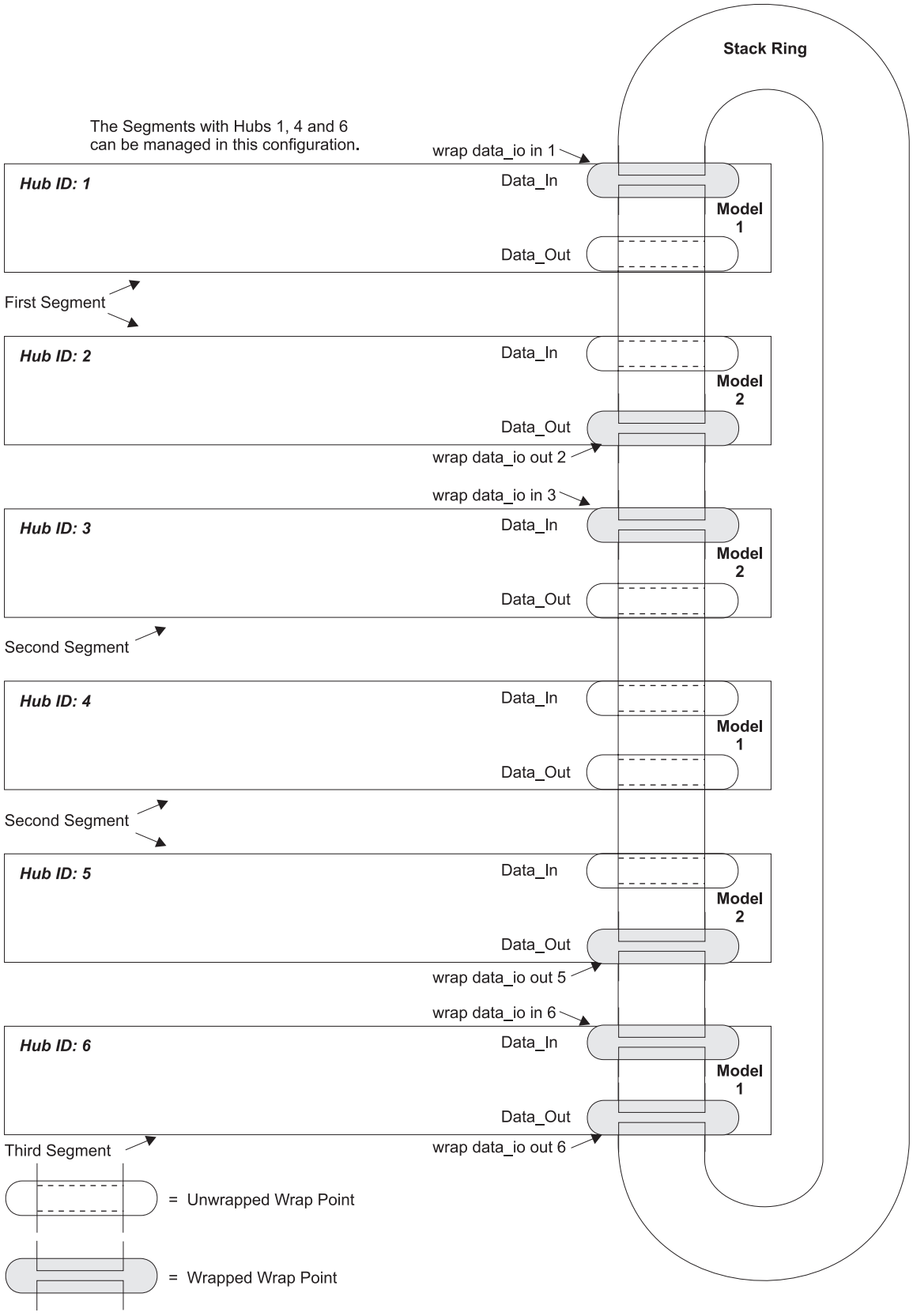

Figure 6-8. Six Units with Three Segments

Chapter 7. 8239 Device Management

In addition to concentrator functions, the 8239 provides both device and network management. This chapter describes these device management functions:

- Connectivity methods
- Updating Operational Code
- Scripts
- Trap processing

Chapter 8, “Network Management” on page 8-1 provides information about the network management functions.

Connectivity Methods

There are two connectivity methods used to physically access the 8239:

- Out-of-band connectivity, in which access to the 8239 is through the EIA-232 port. Both the 8239 Model 1 and Model 2 support out-of-band connectivity.
- In-band connectivity, which is the ability to access the 8239 from a remote station using the token-ring network. Only the 8239 Model 1 supports in-band connectivity.

Out-of-Band Connectivity

The 8239 supports out-of-band access on both models through the EIA-232 port. You can attach either an ASCII terminal for local access or a modem for remote access. See “Connecting an ASCII Terminal or Modem to the EIA-232 Port” on page 2-5 for instructions for connecting to the EIA-232 port. See “Using the Command Interface” on page 4-1 for information about the command interface.

Note: A session on the EIA-232 port does not time out.

In-Band Connectivity

The 8239 supports in-band access on the Model 1 only. The 8239 Model 1 must be configured with an IP address to use in-band connectivity. In-band connectivity is accessed through these protocols:

Telnet
SNMP
PING
TFTP

The use of these protocols with the 8239 is described in the following sections.

Telnet

Use Telnet from an external token-ring station to run a terminal session over an IP network. Up to five users can use Telnet to access an 8239 Model 1 at one time. An idle Telnet session is disconnected after 15 minutes.

Access to the 8239 terminal is controlled by user names and passwords. See “Using the Command Interface” on page 4-1 for information about using the command interface and “Access Modes” on page 7-3 for information about access to the command interface.

SNMP

The 8239 contains an SNMP agent that can communicate with an SNMP manager. The following MIBs are supported by the 8239:

IBM 8239 TR Hub MIB
RMON (RFC 1757)
TR Extensions to RMON (RFC 1513)
RMON 2 (RFC 2021)
RMON MIB Protocols IDs (RFC 2074)
Aspen Config MIB
Trapmib
DLM Mib
ECAM MIB
IEEE 802.5 TR MIB (RFC 1748)
IBM TR Surrogate MIB (AWP-7607)
IBM TR Surrogate Trap MIB (AWP-7607)
MIB II (RFC 1213)

All MIBs supported by the 8239 can be accessed via the 8239 Model 1's IP address.

PING

PING is a useful starting point for verifying connectivity or diagnosing network problems. Use it to test the reachability of IP devices on the network. The 8239 supports:

- Pinging from the 8239 Model 1 to another IP address
- Pinging from an external token-ring station to the 8239 Model 1's IP address

Issuing the PING command at the 8239 terminal prompt results in the 8239 sending 10 Internet Control Message Protocol (ICMP) request packets to the specified device. If the device is active, it should respond to each request packet from the 8239. If the device responds to less than 100% of the request packets, the network may be dropping packets.

If you have trouble pinging a remote device, make sure that:

- The 8239's IP information (IP address, subnet mask, and default gateway) is correct
- The device is on the same network (segment), or bridged or routed to that segment
- The Management Interface is enabled (using the SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE command
- Use the SET MANAGEMENT_INTERFACE ARP_RESOLVE_METHOD command to clear the source routing bit in Address Resolution Protocol (ARP) packets

TFTP

Use the Trivial File Transfer Protocol (TFTP) to transfer files to or from the 8239 Model 1. These types of files can be transferred ***to*** an 8239 Model 1:

- Code
- Configuration setup files
- Scripts

These types of files can be transferred ***from*** an 8239 Model 1:

- Scripts
- Trace files
- Event logs

Access Modes

Access modes prevent unauthorized access to the 8239. For the command interface, access mode is in the form of a user login and password. When using SNMP, the access mode is defined by the community table.

Command Interface

Two access modes are supported for the command interface:

- Administrator
- User

Both of these modes are password-protected.

The tasks that a user can do are a subset of what an administrator can do. The administrator access mode allows you to change parameters that affect connectivity, such as IP information, network assignments, and so on.

SNMP

Access to the 8239 via SNMP is controlled by the use of community names. The 8239 has four levels of access. Each succeeding level is granted the rights of the lower levels in addition to the specific capabilities listed:

- **Level 1** provides read access to MIB-II objects. The default community name is *public*.
- **Level 2** provides read access to MIB-II, RMON MIB, and Aspen MIB objects, excluding objects in the accessControl group and in the captureBufferTable. The default community name is *rmon*.
- **Level 3** provides write access to RMON MIB and Aspen MIB objects, excluding the objects in the probeAdmin, interface, and accessControl groups. It provides read access to MIB-II, RMON MIB (including the captureBufferTable), and Aspen MIB objects excluding those in the accessControl group. It also provides write access to the 8239 MIB, excluding certain groups, such as the community table. The default community name is *user*.
- **Level 4** provides read and write access to all MIBs. The default community name is *admin*.

Access Control List: For additional security, you can specify which IP addresses can access an 8239 with a particular community name. This measure prevents wide access to well-known communities. It is recommended that you set up a script or the BOOTP configuration file to implement this protection.

Updating 8239 Operational Code

This section contains the following information:

- Obtaining 8239 operational code
- Loading 8239 operational code using XMODEM or TFTP

Obtaining New 8239 Operational Code

The 8239 operational code is obtained in a binary file. The files used for the 8239 Model 1 and the 8239 Model 2 are unique files. The Model 1 and Model 2 filenames have a format of m1r*xvy*.opr and m2r*xvy*.opr, respectively, where *x* is the release number and *y* is the version number.

The Model 1 operational code file, which contains both the Model 1 and Model 2 operational code, is loaded on a Model 1; all of the Model 1s and Model 2s in the stack will be updated with the code. The Model 2 operational code file, which contains only the Model 2 operational code, is loaded on a Model 2; all of the Model 2s in the stack will be updated with the code. All 8239s in the same stack should run the same code level.

The most recent 8239 operational code can be obtained by either of these methods:

- Retrieving it from our web site at *http://www.networking.ibm.com/support/8239*
- If the 8239 is under warranty, contact your reseller or call IBM. In the United States, call IBM at 1-800-772-2227; in Canada, call 1-800-IBM-SERV (1-800-426-7378)

  For warranty upgrade or post-warranty maintenance service, call 1-800-IBM-SERV (1-800-426-7378)

If you have a Model 1 in the stack, obtain the Model 1 operational code file; this file contains both the Model 1 and Model 2 operational code. If you have only Model 2s in the stack, obtain the Model 2 operational code file.

Loading New Operational Code

The 8239 Model 1 will update all Model 1s and Model 2 in the stack. The Model 1 operational code file is loaded on the Model 1 using either XMODEM or TFTP. After the code is loaded, the appropriate code is automatically copied to all of the other Model 1s and Model 2s in the stack. To start executing the new code, all of the 8239s in the stack must be reset.

The Model 2 will update only Model 2s in the stack. Load the Model 2 operational code file on the Model 2 using XMODEM. After the code is loaded, the code is automatically copied to all of the other 8239s in the stack. To start executing the new code, all of the 8239 Model 2s in the stack must be reset.

Updating Using XMODEM

To load new code onto your 8239 Model 1 or Model 2 using XMODEM:

1. Put the file containing the new code on the workstation that connects to the 8239 EIA-232 port.
2. Log onto the 8239 using your terminal emulation software.
3. If your terminal baud rate has not been changed from the default value of 9600 bits per second, you may want to configure both the 8239 and the terminal emulation software for a higher baud rate so that the file transfer goes faster.
4. Issue the LOAD OPERATIONAL_CODE XMODEM command.
5. When the message *Ready to RECEIVE File in binary mode* appears, indicate to your terminal emulation software that the file transfer should start. Specify:

- XMODEM or 1K-XMODEM for the protocol. 1K-XMODEM causes the file transfer to occur faster.
- The filename of the file to be transferred.

6. After the file transfer is completed, the 8239 will automatically update the code on the appropriate hubs in the stack. Once the message *Code load complete* appears, the hubs can be reset at any time to execute the new code; for example, you can issue the RESET_HUB ALL command.

Updating Using TFTP

Code can be updated using TFTP on 8239 Model 1s only. The code transfer can be triggered through a terminal interface command or SNMP. Only the instructions for updating code using the terminal interface are described here.

1. Put the file containing the new code on your TFTP server. Make sure that the permission code for the file allows read-access for "others". For example, on AIX or UNIX systems, specify `chmod o+r` *file*, where *file* is the name of the file to be transferred.
2. Log onto the 8239 using either your terminal emulation software or Telnet.
3. Issue the LOAD OPERATIONAL_CODE TFTP command, specifying the TFTP server's IP address and the filename of the file to be transferred.
4. After the file transfer is done, the 8239 will automatically update the code on all other hubs in the stack. Once the message *Code load complete* appears, the hubs can be reset at any time to execute new code; for example, you can issue the RESET_HUB ALL command.

Scripts

A script is an ASCII file containing a list of commands that can be issued from the 8239 terminal interface. Scripts allow you to:

- Execute a set of commands by issuing one command instead of typing all the commands
- Define a set of commands prior to actually executing them (for example, for preconfiguring stack units)

You can create or modify script files in real-time on all 8239 stack units. You can transfer script files into or out of all stack units:

- Using XMODEM via the stack unit's local EIA-232 port
- Using TFTP to the stack unit's IP address
- By downloading from a BOOTP server

Script files that are created using the terminal interface or that are downloaded via TFTP are retained after a reset. All stack units can execute scripts when invoked by a user command through a terminal interface. Only the 8239 Model 1 supports scheduling a script, which means that the script is executed by time of day. When a script is downloaded using BOOTP, it is automatically executed after the download completes.

The script interface, unlike the command interface, provides no interactive syntax checking. When a script is created or updated, no checking is done to ensure that:

- The command syntax is valid

- The specified hub IDs exist
- The appropriate access mode exists for command execution

If an error is detected during the execution of a script, the remaining lines in the script are not executed.

Each script file can contain up to 25 lines; each line can contain up to 72 characters. A script can contain comments that are ignored when the script is executed. Each comment line counts toward the maximum number of lines in a script. Comment lines begin with #; all characters after the # to the end of the line are ignored.

Creating Scripts

Follow the steps in the example in this section to create a script.

Creating a Script Name

The first task in creating a script is to choose a name and attach it to a *script index*. Once the script has a name, you can add commands, modify commands, delete commands, and run the script by using this name.

Assume that there are currently no scripts defined. To create a script named *script1*, type:

```
>>script <Enter>
```

The script interface displays accepted inputs:

```
Accepted inputs:

1) -NoName-1                  6) -NoName-6
2) -NoName-2                  7) -NoName-7
3) -NoName-3                  8) -NoName-8
4) -NoName-4                  9) -NoName-9
5) -NoName-5                  10) -NoName-10

>>script
```

You must choose one of the 10 available script index numbers. Type:

```
>>3 <Enter>
```

The script interface replaces the number you typed with the name currently assigned to the third script and positions you at the end of the command:

```
>>script  -NoName-3
```

For a list of possible inputs, type **?** and press **Enter**.

```
Accepted inputs:

1) add                       6) insert
2) clear                     7) list
3) copy_to                   8) name
4) delete                    9) replace
5) edit                     10) run

>>script -NoName-3
```

To name the script, type:

```
>>script -NoName-3 _name <Enter>
```

The script interface responds:

```
Enter Script Name (Max 15 characters):

>> script _NoName-3 name
```

Enter the name of the script:

```
>> script _NoName-3 name_script1 <Enter>
```

To display the script name, type:

```
>>display scripts <Enter>

1) -NoName-1                6) -NoName-6
2) -NoName-2                7) -NoName-7
3) script1                  8) -NoName-8
4) -NoName-4                9) -NoName-9
5) -NoName-5                10) -NoName-10
```

Adding Commands

It is recommended that you first manually execute commands that you are going to put in a script to verify that the syntax is correct. Assume you are at hub 1 and that you wish to use a script to disable ports 3, 5, and 10. To disable port 3, type

```
>>disable port 1.3 <Enter>
```

To check the command, type:

```
>>display port 1.3 <Enter>

                                  8228              Speed    Counters
 Port   Mode     Status           Mode    Traps     Detect   Spd  Bcn
 ----   ------  ----------       -------  -------   ------  ---  ---
 1.3  Disabled  No Phantom      Disabled  Disabled  Enabled   0    0
```

Before adding commands to the script, verify that the script is empty:

```
>>script script1 list <Enter>

Script: script1
[Empty]
>>
```

The **add** command positions you at the end of the script. When you press **Enter**, a new line is automatically created. Press the **Esc** key to terminate the **add** command. To create a script to disable the three ports, type:

```
>>script script1 add <Enter>

Enter commands . . . <ESC> to quit

[ 1]  disable port 1.3 <Enter>
[ 2]  disable port 1.5 <Enter>
[ 3]  disable port 1.10 <Enter>
[ 4]  <Esc>
```

To look at the script, type:

```
>>script script1 list <Enter>
```

```
Script: script1
[ 1]  disable port 1.3
[ 2]  disable port 1.5
[ 2]  disable port 1.10

>>
```

Editing Scripts

Continuing the example from “Adding Commands” on page 7-7, assume you need to disable port 6 instead of port 5.

Because you will access lines within the script by line number, you should list the script before you modify it.

```
>>script script1 list <Enter>
```

The script interface responds:

```
Script: script1
[ 1]  disable port 1.3
[ 2]  disable port 1.5
[ 3]  disable port 1.10

>>
```

To look at your choice of command options, type:

```
>>script script1 <Enter>

Accepted inputs:

1) add                      6) insert
2) clear                    7) list
3) copy_to                  8) name
4) delete                   9) replace
5) edit                    10) run

>>script script1
```

To replace line 2 to reflect hub 6 rather than hub 5, type:

```
>>script script1 _edit 2 <Enter>

[ 2]  disable port 1.5
```

Change the 5 to a 6.

To verify the change, type:

```
>> script script1 list <Enter>

Script: script1
[ 1]  disable port 1.3
[ 2]  disable port 1.6
[ 3]  disable port 1.10

>>
```

Running Scripts

You can run a script:

- From the command line
- From a schedule
- From an RMON event

From the Command Line

To start a script from the command line, type:

```
script script1 run <Enter>
```

Note that:

- Output generated by the script is displayed at the terminal where the command was entered.
- Output that prompts you to press any key to continue does not stop the script running; the script continues to completion. The output may appear erratic because of screen buffer overrun.
- Scripts can be chained; that is, one script can end with a command that runs another script. Be careful that you do not create a loop that would cause you to have to reset the 8239.

From a Schedule (8239 Model 1 only)

To run a script from a schedule, follow these steps.

Create the Script: Follow the steps in "Creating Scripts" on page 7-6 to create a script. Make a note of the index number of your script, as it is used by the scheduler.

Determine a Schedule Index: The scheduling function operates by keeping track of a schedule index. Type:

```
>>display schedule all<Enter>
```

In this example, the script interface displays an empty schedule:

```
Schedule                  Script            Days
Index     Mode        Time      Number      SMTWTFS     Dates
-----    -----        ----      ------      --------    -----
  1      disabled     00:00     *****
  2      disabled     00:00     *****
  3      disabled     00:00     *****
  .
  .
  .
 19      disabled     00:00     *****
 20      disabled     00:00     *****
```

In this example, an item is added to index 1.

Define the Schedule: Assume that you want to run the script script1 every weekday at 13:00 hours.

```
>>set schedule <Enter>

Accepted inputs:

 1) script
 2) interval
 3) month_periodic
 4) day_periodic
 5) date

>> set schedule
```

To perform a task every weekday, choose **4) day_periodic**. You can type the command or type the number of the command, **4**.

```
>> set schedule 4 <Enter>
 Enter Schedule #(1-20):

>> set schedule day_periodic 1 <Enter>
Accepted inputs:

 1) Mon                          6) Sat
 2) Tue                          7) Sun
 3) Wed                          8) Weekdays
 4) Thr                          9) Weekends
 5) Fri                         10) Everyday

>> set schedule day_periodic 1
```

To run the schedule on weekdays, type:

```
>> set schedule day_periodic 1 8 <Enter>

Enter the time(hh:mm):

>> set schedule day_periodic 1 Weekdays
```

Provide the time:

```
>> set schedule day_periodic 1 Weekdays 13:00 <Enter>


Schedule                  Script           Days
Index     Mode        Time      Number      SMTWTFS     Dates
-----    -----        ----      ------      --------    -----
  1      disabled     13:00+    *****
```

You have now specified when you want to run the script.

Attach the Script: You next need to specify the script you want to run.

```
>> set schedule script <Enter>
Accepted inputs:

1) -NoName-1                6) -NoName-6
2) -NoName-2                7) -NoName-7
3) script1                  8) -NoName-8
4) -NoName-4                9) -NoName-9
5) -NoName-5                10) -NoName-10
```

Provide the name of your script:

```
>> set schedule script script1 <Enter>
 Enter Schedule #(1-20):

>> set schedule script script1
```

Select index **1**:

```
>> set schedule script script1 1 <Enter>

Schedule                  Script           Days
Index     Mode        Time      Number      SMTWTFS     Dates
-----    -----        ----      ------      --------    -----
  1      disabled     13:00+       3         +++++
```

Enable the Script: To enable the script, type:

```
>> enable schedule 1 <Enter>

Schedule                  Script            Days
Index     Mode        Time      Number      SMTWTFS     Dates
-----    -----        ----      ------      --------    -----
  1      enabled      13:00+       3         +++++
```

The schedule is now enabled.

Note:

- Any output generated by a scheduled script will appear at the terminal attached to the EIA-232 port.
- Output that prompts you to press any key to continue does not stop the script running; the script continues to completion. The output may appear erratic because of screen buffer overrun.
- Traps are generated for script completions and script failures. After a scheduled script is executed (on an 8239 Model 1 only), an Execute Script Trap may be sent depending on the script trap_setting. The default value is enabled. To change the script trap_setting, issue ENABLE/DISABLE TRAP_SETTING SCRIPT. To display the current setting, issue DISPLAY TRAP_SETTINGS. For more information about traps, refer to “Trap Processing” on page 7-12.

From an RMON Event (8239 Model 1 only)

To run a script from an RMON event, follow these steps.

Create the Script: Follow the steps in “Creating Scripts” on page 7-6 to create a script. Make a note of the index number of your script, as it is used by the scheduler.

Set Up RMON Alarms and Events: Use the terminal interface or SNMP. Make a note of the event index, as it is used by the Event Table.

Assume the event index is 14 for this example.

Attach the Event to the Script: Type:

```
>> set event_script <Enter>
```

The command interface responds:

```
Accepted inputs:

1) -NoName-1                  6) -NoName-6
2) -NoName-2                  7) -NoName-7
3) script1                    8) -NoName-8
4) -NoName-4                  9) -NoName-9
5) -NoName-5                  10) -NoName-10

>> set event_script script1 <Enter>

Enter Event Number:
```

Type your event index number:

```
>> set event_script script1 14 <Enter>
Event 14 will run script 3
```

Note:

- You must name a script before attaching it to an event.
- Event numbers must be unique. Only one event of a particular number will be listed in the table; duplicates are deleted. While several different events may trigger the same script, several scripts cannot be triggered by a single event.
- You can attach up to 50 events. When the script event table is full, you must clear space using the CLEAR EVENT_SCRIPT command.
- Any script output appears ***only*** at the terminal attached to the EIA-232 port.
- The Event Table always returns information referencing the script index, not the script name.

Trap Processing

Traps are unsolicited notifications of events detected or caused by the 8239. They provide information about significant events about the stack or your network. They can be used to trigger an administrator action, if desired.

Based on the settings of trap flags, the 8239 will send a predefined set of traps associated with various MIBs that the 8239 supports. You can configure the 8239 to display the trap, send the trap, or both display and send the trap to a trap receiver defined in an 8239 Model 1's trap community table. All 8239s forward 8239-specific traps using intrastack communications on the control ring to any 8239 Model 1s in the stack. These 8239-specific traps are displayed or sent to a trap receiver based on the configuration settings of the 8239 Model 1. The 8239 trap utility provides you the flexibility to:

- Have a single point to monitor the traps or to send the traps to an SNMP application
- Choose to have trap information disseminated to multiple trap receivers
- Have a specific 8239 Model 1 handle one set of traps and another Model 1 handle another set of traps

You can configure traps or access trap information using one of the following methods:

- A terminal interface command using the EIA-232 interface
- A terminal interface command using a Telnet session to an 8239 Model 1 in the stack
- An SNMP request to the appropriate object in the 8239 MIB issued to an 8239 Model 1 in the stack

Instructions for accessing information in the remainder of this chapter describe only access through the terminal interface command.

Methods of Viewing Traps

The methods by which you can view trap information are:

- Displaying the trap on the terminal interface (EIA-232 interface or, on an 8239 Model 1 only, a Telnet session)
- Storing the trap in a trap log that can be displayed on your request
- Displaying the trap on the LCD (8239 Model 1 only)
- Sending the trap to an SNMP application (8239 Model 1 only)

The method used is governed by the 8239 configuration settings referred to as *trap flags*. For further information about trap flags, see “Configuring for Trap Generation and Accessing Trap Information” on page 7-14.

Displaying Traps on the Terminal Interface

You access the 8239 terminal command interface by logging in via the 8239’s EIA-232 interface or a Telnet session. Telnet is supported by the 8239 Model 1 only. For more information on the terminal interface, refer to “Using the Command Interface” on page 4-1. You can display traps at a remote console that is connected by either the EIA-232 interface or a Telnet session.

To display traps on the terminal interface you must configure the 8239 with console_display enabled. The factory setting for console_display is enabled. To change the console_display setting, issue the ENABLE/DISABLE TRAP_SETTING CONSOLE_DISPLAY terminal interface command. To display the current setting for console_display, issue the DISPLAY TRAP_SETTINGS terminal interface command. Even when console_display is enabled, other trap flag settings can prevent the trap from being displayed.

Logging Traps

Each 8239 stores traps in a log that is maintained locally so that a history of the traps that were generated can be obtained easily. The trap log contains up to 64 of the most recent traps that were generated.

Only the traps that have their associated trap flag enabled are stored in the trap log. For example, all of the items listed under DISPLAY TRAP_SETTINGS except for "console_display" are considered to be trap flags. For more information about the individual trap flags, refer to “Configuring for Trap Generation and Accessing Trap Information” on page 7-14.

To display the trap log, issue the DISPLAY TRAP_LOG terminal interface command. The trap log is cleared whenever the 8239 is reset or the CLEAR TRAP_LOG terminal interface command is issued.

Displaying Traps on the 8239 Model 1 LCD

A small subset of the possible traps that the 8239 can generate are displayed on the 8239 Model 1 LCD. These traps are listed in “Operational Codes” on page 5-15.

The trap is displayed on the LCD only if the individual trap flag for that trap is enabled. For more information about the individual trap flags, refer to “Configuring for Trap Generation and Accessing Trap Information” on page 7-14.

The 8239 refreshes the LCD every 2 seconds with the last trap that was generated. If multiple traps occur before the LCD is refreshed, only the last trap is displayed. A trap remains on the LCD display until a subsequent trap overwrites it.

Sending the Traps to an SNMP Application (8239 Model 1 only)

A trap that is sent via SNMP enables a management application to interpret the trap and provide different mechanisms for alerting the user about the event. When a trap is generated, the 8239 Model 1 sends the trap via SNMP if there is a valid entry in the 8239's trap community table. The trap community table defines the IP addresses to which traps will be sent. It can contain up to 30 entries.

There are no entries configured in the trap community table at the factory. To add entries to the trap community table, issue the SET TRAP_COMMUNITY terminal interface command. To control the IP addresses to which traps are sent, you must use one of these parameters in the SET TRAP_COMMUNITY command:

- **all** to send all generated traps to the specified IP address
- **tr_surrogate** to send the IBM TR Surrogate MIB traps (CRS, REM, RPS) to the specified IP address
- **ibm8239** to send the 8239 MIB traps to the specified IP address
- **rmon** to send RMON alarms to the specified IP address
- **mib2** to send MIB II traps to the specified IP address

To clear entries in the trap community table, issue the CLEAR TRAP_COMMUNITY terminal interface command.

Configuring for Trap Generation and Accessing Trap Information

The 8239 can generate the following types of traps:

- 8239-specific traps
- IBM Token-Ring Surrogate traps
- MIB II traps
- RMON alarms

Some of the traps have trap flags associated with them so that you can control whether the traps are displayed or sent. The following sections describe each type of trap.

8239-Specific Traps

All 8239-specific traps are forwarded to any 8239 Model 1 in the stack for additional processing. 8239-specific traps can be divided into groups according to whether the traps have associated trap flags.

Traps That Have Multiple Flags

Port Security Intruder Detected Trap: When port security is enabled for a port, the default value for action_on_intrusion is *trap_only*, which means that a trap will be generated on an intrusion. To change the setting, issue the SET SECURITY_PORT ACTION_ON_INTRUSION terminal interface command. To display the current setting, issue the DISPLAY SECURITY PORT terminal interface command. For more information about port security, refer to "Port Security" on page 6-7.

Another trap flag associated with the Security Intruder Detected trap, TRAP_SETTING SECURITY_INTRUDER, enables the trap to be displayed. The default value for this flag is enabled. To change the setting, issue the ENABLE/DISABLE TRAP_SETTING terminal interface command. To display the current setting, issue the DISPLAY TRAP_SETTINGS terminal interface command.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If the console_display TRAP_SETTING is enabled, the trap will be displayed on the terminal interface. Otherwise, nothing is displayed.
- **Trap Log**: The trap is put in the trap log.
- **8239 Model 1 LCD**: The trap is not displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table.

  The factory setting for the trap community table is null. To specify where 8239-specific traps should be sent, issue the SET TRAP_COMMUNITY IBM8239 terminal interface command.

Port Up/Down Trap: The default value for Port Up/Down traps is enabled. To change the setting, issue the ENABLE/DISABLE PORT_SETTING TRAPS terminal interface command. To display the current setting, issue the DISPLAY PORT terminal interface command. Port up/down traps are generated whenever PORT_SETTING TRAPS is enabled for that port.

Another trap flag associated with the Port Up/Down trap, TRAP_SETTING PORT_UP_DOWN, enables the trap to be displayed. The default value for this flag is enabled. To change the setting, issue the ENABLE/DISABLE TRAP_SETTING PORT_UP_DOWN terminal interface command. To display the current setting, issue the DISPLAY TRAP_SETTINGS terminal interface command.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If the console_display TRAP_SETTING is enabled and the port_up_down TRAP_SETTING is enabled, then the trap will be displayed on the terminal interface. Otherwise, nothing is displayed.
- **Trap Log**: The trap is put in the trap log if the port_up_down TRAP_SETTING is enabled.
- **8239 Model 1 LCD**: The trap is not displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table and the port_up_down TRAP_SETTING is enabled.

  The factory setting for the trap community table is null. To specify where 8239-specific traps should be sent, issue the SET TRAP_COMMUNITY IBM8239 terminal interface command.

Traps That Have a Single Flag: The following traps are associated with the hub:

- Control IO Status Up/Down
- Multiple Users
- Port Up/Down
- Ring IO Status Up/Down (8239 Model 1 only)
- Script

Each of these traps has an associated trap flag. The default value for each of these flags is enabled. To change the setting, issue the ENABLE/DISABLE TRAP_SETTING terminal interface command. To display the current setting, issue the DISPLAY TRAP_SETTINGS terminal interface command.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If the console_display TRAP_SETTING is enabled and the associated flag for this trap in TRAP_SETTING is enabled, then the trap will be displayed on the terminal interface. Otherwise, nothing will be displayed.
- **Trap Log**: The trap is put in the trap log if the associated flag for this trap in TRAP_SETTING is enabled.
- **8239 Model 1 LCD**: Control IO Status Up Down, Data IO Status Up Down, and Ring IO Status Up Down are displayed on the LCD, but Multiple Users and Script are not.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table and the associated flag for this trap in TRAP_SETTING is enabled.

  The factory setting for the trap community table is null. To specify where 8239-specific traps should be sent, issue the SET TRAP_COMMUNITY IBM8239 terminal interface command.

Traps That Have No User-Configured Flags: The following traps cannot be disabled:

- Code Version Mismatch
- Hub Up/Down

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: The trap is always displayed on the terminal interface.
- **Trap Log**: The trap is put in the trap log.
- **8239 Model 1 LCD**: Hub Up/Down and Code Version Mismatch are displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table.

  The factory setting for the trap community table is null. To specify where 8239-specific traps should be sent, issue the SET TRAP_COMMUNITY IBM8239 terminal interface command.

IBM Token-Ring Surrogate Traps

CRS, REM, and RPS can generate traps. Each server has a trap flag that indicates whether or not a trap should be generated. The factory setting for CRS, REM, and RPS is to generate traps.

To change the trap flag setting for CRS, issue the ENABLE/DISABLE TR_SURROGATE CRS_TRAPS terminal interface command. To display the current trap flag setting, issue the DISPLAY TR_SURROGATE CRS_STATUS terminal interface command.

To change the trap flag setting for REM, issue the ENABLE/DISABLE TR_SURROGATE REM_STATUS REM_TRAPS terminal interface command. To

display the current trap flag setting, issue the DISPLAY TR_SURROGATE REM_STATUS terminal interface command.

To change the trap flag setting for RPS, issue either the ENABLE/DISABLE TR_SURROGATE RPS_TRAPS or the SET MANAGEMENT_INTERFACE RPS_TRAPS terminal interface command. To display the current trap flag setting, issue either the DISPLAY TR_SURROGATE RPS_STATUS terminal interface command or the DISPLAY MANAGEMENT_INTERFACE terminal interface command.

CRS, REM, and RPS traps are not forwarded to other 8239 Model 1s in the stack.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If the console_display TRAP_SETTING is enabled, then the trap is displayed on the terminal interface. Otherwise, nothing is displayed.
- **Trap Log**: The trap is put in the trap log.
- **8239 Model 1 LCD**: The trap is not displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table.

  The factory setting for the trap community table is null. To specify where CRS, REM, or RPS traps should be sent, issue the SET TRAP_COMMUNITY TR_SURROGATE terminal interface command.

MIB II traps

The 8239 Model 1 sends out the following MIB II traps:

- Authentication
- Warm Start

Warm Start traps are always generated. Authentication traps are only generated when the authentication TRAP_SETTING flag is enabled. The default value for the authentication trap flag is enabled.

To change the setting, issue the ENABLE/DISABLE TRAP_SETTING AUTHENTICATION terminal interface command. To display the current setting, issue the DISPLAY TRAP_SETTINGS command.

MIB II traps are not forwarded to other 8239 Model 1s in the stack.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If the console_display TRAP_SETTING is enabled, then the trap will be displayed on the terminal interface. Otherwise, nothing is displayed.
- **Trap Log**: The trap is put in the trap log.
- **8239 Model 1 LCD**: The MIB II traps are not displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the trap community table.

  The factory setting for the trap community table is null. To specify where MIB II traps should be sent, issue the SET TRAP_COMMUNITY MIB2 terminal interface command.

RMON Alarms

"Remote Monitoring: RMON, RMON 2, ECAM" on page 8-5 discusses what action can be taken when an RMON event occurs. The following sections describe what takes place if you specified that a trap should be generated. All of these actions are on the local hub only; RMON traps are not forwarded to other 8239 Model 1s in the stack.

If the trap is generated, viewing takes these forms:

- **Terminal Interface**: If console_display in the Trap Settings is enabled and the RMON flag in the Trap Settings is enabled, then the trap will be displayed on the terminal interface. Otherwise, nothing is displayed.
- **Trap Log**: The trap is put in the trap log.
- **8239 Model 1 LCD**: The trap is not displayed on the LCD.
- **Sent to an SNMP Application**: The trap is sent via SNMP if there is a valid entry in the RMON trap community table. Most RMON managers, like ReMon, set up a trap community entry in the RMON 2 trap community table. An entry also can be added to the RMON 2 trap community table by issuing an SNMP Set request to the appropriate object in the 8239 MIB or by issuing the SET TRAP_COMMUNITY RMON terminal interface command. All entries in the RMON 2 trap community table can be displayed using the RMON 2 MIB. The 8239 MIB or the DISPLAY COMMUNITY terminal interface command only display the RMON 2 entries that were added using the 8239 MIB or the SET TRAP_COMMUNITY RMON command.

MAC Addresses

Each 8239 is assigned a set of MAC address at the time of manufacture. The first MAC address in the set is referred to as the *base MAC address*. You can identify this base MAC address using one of the following commands:

- DISPLAY HUB
- DISPLAY INVENTORY
- DISPLAY STACK

The base MAC address is also identified on a label on the front left side of the 8239 shipping carton and on the front left side of the 8239 itself.

On the 8239 Model 1, the burned-in MAC address assigned to the Management Interface is the Model 1's base MAC address. Issue an SNMP Get request to the appropriate object in the 8239 MIB or issue the DISPLAY MANAGEMENT_INTERFACE terminal interface command to view the burned-in MAC address of the Management Interface.

On both the 8239 Model 1 and the 8239 Model 2, MAC addresses are assigned to the hardware-assist entities used for beacon recovery or address-to-port mapping. Issue an SNMP Get request to the appropriate object in the 8239 MIB or issue the DISPLAY HUB terminal interface command to see these addresses.

Chapter 8. Network Management

The 8239 contains network management functions to assist in managing networks and providing information that can help you analyze and optimize your network's performance, prevent outages, and troubleshoot problems. Token-Ring media management as well as higher-layer protocol management is supported. Network management support is provided only by the 8239 Model 1. Information is provided for a network only when the 8239 Model 1's Management Interface is inserted into the network being monitored.

This chapter contains information on how to access the network management data from an 8239 Model 1 and provides details about the following network management functions that are supported by the 8239 Model 1:

- IEEE 802.5 Token Ring MIB (RFC 1748)
- MIB II (RFC 1213)
- Remote Monitoring (RMON)
  - RMON MIB (RFC 1757)
  - Token Ring Extensions to the RMON MIB (RFC 1513)
- RMON 2
  - RFC 2021
  - RMON MIB Protocol Ids (RFC 2074)
- Enterprise Communications Analysis Module (ECAM)
- IBM Token Ring Surrogate MIB and Surrogate Trap MIB
  - Configuration Report Server (CRS)
  - Ring Error Monitor (REM)
  - Ring Parameter Server (RPS)

For a complete listing of commands referenced in this chapter, see the *Command Reference*.

Accessing Network Management Data

You can use in-band and out-of-band access to the 8239 Model 1 to configure it to support the various network management functions and to obtain the network management information from the Model 1.

- In-band access is provided via:
  - A Telnet session using the terminal interface
  - SNMP using the appropriate MIB

  To configure the 8239 Model 1 for in-band connectivity, refer to "Configuring the 8239 for In-Band Connectivity" on page 4-5.
- Out-of-band access is provided through the EIA-232 connection using the terminal interface. To configure the 8239 Model 1 for out-of-band connectivity, refer to "Out-of-Band Connectivity" on page 7-1.

The network management information collected and analyzed by the 8239 Model 1 can be obtained directly only from the Model 1 that is monitoring the network. A request for network management information cannot be issued to one 8239 Model 1 to retrieve information from another Model 1 in the same stack. To obtain the network management information from an 8239 Model 1, the request must come from either that Model 1's EIA-232 interface (out-of-band access) or via a

Token-Ring workstation that has a physical path to the network that the Model 1 is monitoring (in-band access).

IEEE 802.5 Token Ring MIB (RFC 1748)

Use the IEEE 802.5 MIB (RFC 1748) to obtain information about a specific Token-Ring interface. This MIB collects information for the 8239 Model 1's Management Interface, as opposed to information about all the stations on the network that the Model 1 is monitoring.

The 8239 Model 1 supports the following tables in the 802.5 MIB:

- The Interface Table, which tracks the state of the 802.5 interface and some of the characteristics associated with the 802.5 interface
- The Statistics Table, which tracks statistics and MAC-level error counters for the 802.5 interface

Configuring the 8239 Model 1 to Support the 802.5 MIB

Whenever the 8239 Model 1 is operational, the 8239 will automatically provide information from the Interface Table. To collect data for the Statistics Table, the 8239 Model 1 must be configured to do so. Configure the 8239 Model 1 using the SET MANAGEMENT_INTERFACE 802.5_GROUP terminal interface command or by issuing an SNMP Set request to the appropriate object in the IBM 8239 TR Hub MIB (*8239 MIB*).

The factory default for 802.5_GROUP is DISABLED, which means that all of the entries in the Statistics Table are set to 0. To allow the 8239 Model 1 to increment the counters in the Statistics Table, issue the SET MANAGEMENT_INTERFACE 802.5_GROUP ENABLE command or issue an SNMP Set request to the appropriate object in the 8239 MIB.

Accessing 802.5 Information

The 802.5 Interface Table and Statistics Table can be obtained by the following methods:

- SNMP using the IEEE 802.5 MIB (OID dot5 of 1.3.6.1.2.1.10.9)
- Terminal interface using the DISPLAY COUNTER 802.5 command

The 8239 Model 1 does not support the dot5LastBeaconSent object in the Interface Table.

Interface Table

The Interface Table contains some objects that are defined to have read/write access in the 802.5 MIB, but all of the read/write objects in the 802.5 MIB are supported as read-only in the 8239. The "write" action described in the 802.5 MIB can be performed using an IBM private MIB or the 8239 terminal interface. The read/write objects in the 802.5 MIB are listed here, along with the corresponding 8239 request you can use to accomplish the same action:

- dot5Commands

  The dot5Commands are Nop, Open, Close, and Reset. The 8239 does not support a Nop function.

There are no specific 8239 commands to tell the Management Interface to open or close. The Management Interface will close and then reopen as a result of issuing an 8239 terminal interface command or an SNMP Set request to the appropriate MIB. The terminal interface commands and the corresponding MIBs that make the Management Interface close and then reopen are:

SET MANAGEMENT_INTERFACE ADMINISTRATIVE_MODE	8239 MIB
SET MANAGEMENT_INTERFACE EARLY_TOKEN_RELEASE	8239 MIB
SET MANAGEMENT_INTERFACE LOCALLY_ADMIN_ADDRESS	8239 MIB
SET MANAGEMENT_INTERFACE MAC_ADDRESS_TYPE	8239 MIB
SET TR_SURROGATE SEGMENT_NUMBER	IBM TR Surrogate MIB

Use the DISPLAY MANAGEMENT_INTERFACE command to view the current values for the Management Interface.

To reset the Management Interface, a reset must be issued to the hub by using the RESET_HUB command or an SNMP Set request to the appropriate object in the IBM 8239 MIB.

- dot5RingSpeed

  To change the Management Interface's ring speed, which also changes the ring speed associated with all of the ports on the hub, issue the SET HUB RING_SPEED command or an SNMP Set request to the appropriate object in the 8239 MIB.

- dot5ActMonParticipate

  To configure the Management Interface to participate in Active Monitor Contention if the opportunity arises, issue the SET MANAGEMENT_INTERFACE ACTIVE_MONITOR_PARTICIPATION command or an SNMP Set request to the appropriate object in the 8239 MIB.

- dot5Functional

  The only functional addresses supported by the Management Interface that can be changed are the CRS, REM, and RPS functional addresses. Refer to "Configuring for the Surrogate Agent" on page 4-8 for information about changing Management Interface functional addresses.

dot5Upstream and dot5Functional are only valid when dot5RingState has a value of "opened".

Statistics Table

Using the terminal interface only, the 8239 enables you to clear the Statistics Table using the CLEAR COUNTER 802.5 command. This command sets the Statistics Table counters to 0 so that the counters reflect the values since the last CLEAR COUNTER 802.5 command was issued. Clearing the counters lets you see how much the counters have incremented during a period of time. The CLEAR COUNTER 802.5 command has no effect on the values of the counters obtained via SNMP.

MIB-II (RFC 1213)

The 8239 Model 1 supports the following MIB-II groups:

- System group

  The System group (OID 1.3.6.1.2.1.1) provides textual descriptions of the 8239 Model 1 in printable ASCII characters.

- Interfaces group

  The Interfaces group contains characteristics of the Token-Ring interface as well as packet-level statistics related to receiving and transmitting frames at the Token-Ring interface. The Interface statistics collected are for the 8239 Model 1's Management Interface, as opposed to information for all station on the network that the Model 1 is monitoring. When any RMON group is enabled,[1] the Management Interface is receiving all packets on the ring, even those not addressed to it; this fact is reflected in the Receive counters in the Interfaces group.

Note: The 8239 Model 1 does not support the MIB-II IP group, but the information provided by the ipNetToMediaTable is supported in the Model 1 by:

- Using the DISPLAY IP ARP_CACHE command, or
- Accessing the appropriate object in the 8239 MIB.

Configuring the 8239 Model 1 to Support MIB-II

The 8239 Model 1 will automatically collect and provide information for the MIB-II groups that it supports. There are no configuration parameters to enable or disable for this support.

Accessing MIB II Information

The MIB-II System group and Interfaces group can be obtained by the following methods:

- SNMP using the MIB-II MIB
- The terminal interface. Only a subset of the MIB-II System group and Interfaces group is available through the terminal interface.

When you access the information through the terminal interface, the following commands are associated with each MIB-II group listed:

- System Group

sysObjectId	Not available through the terminal interface
sysUpTime	DISPLAY HUB
sysContact	DISPLAY MANAGEMENT_INTERFACE
sysName	DISPLAY MANAGEMENT_INTERFACE
sysLocation	DISPLAY MANAGEMENT_INTERFACE
sysDescription	DISPLAY MANAGEMENT_INTERFACE
sysServices	Not available through the terminal interface

[1] Use DISPLAY MANAGEMENT_INTERFACE to look at the value of RMON group.

- Interfaces Group

  Only the ifIn statistics and the ifOut statistics in the Interfaces Group are available via the terminal interface; issue the DISPLAY COUNTER MIB2_INTERFACE command.

  You can clear the counters in the Interfaces group using the CLEAR COUNTER MIB2_INTERFACE command. This command sets the ifIn and ifOut counters to 0 so that the counters displayed (using DISPLAY COUNTER MIB2_INTERFACE) reflect the values since the last CLEAR COUNTER MIB2_INTERFACE command was issued. Clearing the counters lets you see how much the counters have changed during a period of time. The CLEAR COUNTER MIB2_INTERFACE command has no effect on the values of the counters obtained via SNMP.

Remote Monitoring: RMON, RMON 2, ECAM

The Remote Monitoring (RMON) MIBs defined by the Internet Engineering Task Force (IETF) allow a device to act like a network traffic analyzer monitoring flows and gathering data for all traffic on the network with varying degrees of detail. This data can be obtained remotely by an SNMP-based network management station, referred to as an RMON manager, or through RMON Management Software. A device that supports gathering and reporting the RMON data is referred to as an *RMON probe* or *RMON agent*. The 8239 Model 1 is an embedded RMON probe.

RMON consists of RFC 1757 and RFC 1513. It provides utilization information, packet statistics, and statistics on a MAC-address basis. To get statistics above OSI Layer 2 (the data link layer), RMON 2 was developed. RMON2 lets you track network usage by protocol, and application and traffic patterns can be viewed at the network level (OSI Layer 3).

ECAM was developed from a preliminary version of RMON2 before RMON2 became a standard.

RMON

RMON, sometimes referred to as RMON 1 to distinguish it from RMON 2, consists of the following MIBs:

- RMON MIB (RFC 1757)
- Token Ring Extensions to the RMON MIB (RFC 1513)

The RMON groups are:

- **Statistics**: Contains cumulative traffic and error statistics. It consists of the following groups:
  - **MAC-Layer Statistics**: Collects information from the MAC frames on the ring, including error reports for the ring.
  - **Promiscuous Statistics**: Collects usage statistics from user data (non-MAC) packets.
- **History**: Generates reports from periodic traffic sampling that are useful for analyzing trends. This group also collects utilization and error statistics for MAC-layer history and Promiscuous history.

- **Host**: Tracks statistics associated with each host on the network on a MAC-address basis. This group also contains the order in which the stations are discovered.
- **Host Top N**: Indicates which hosts are top traffic contributors in a given category during a given time frame. Use this object to pinpoint trouble spots, for example, the station sending out the most broadcast frames. This group requires the Host group.
- **Matrix**: Stores statistics about conversations between pairs of MAC addresses.
- **Event**: Controls the actions that are taken when an event occurs. RMON event s occur when:
  - A threshold (alarm) is exceeded
  - A filter that was created matches a packet

  The 8239 Model 1 can respond to an event by:
  - Logging the event
  - Generating a trap
  - Logging the event and generating a trap
  - Doing nothing, that is, using the event as a placeholder or to reset a threshold
- **Alarm**: Enables you to define and set thresholds for various counters. Thresholds can be passed in either a rising or falling direction on existing MIB objects, primarily those in the Statistics group. An alarm is triggered when a threshold is crossed and the alarm is passed to the Event group. The Alarm group requires the Event group.
- **Filter**: Instructs the 8239 Model 1 to capture only those packets that match a specific criterion. This group enables you to configure specific packet capture criteria, for example, packets representing a particular protocol, such as IP, IPX, SNA, or a specific MAC address.
- **Packet Capture**: Captures and uploads to the remote RMON Management software the packets the 8239 Model 1 collected. This group requires the Filter group.
- **Ring-Station**, **Ring-Station Order**, and **Ring-Station Configuration** groups: Provide Token-Ring status, error, and statistics for each active station on the segment being monitored. These groups track the order s of the station on the segment and actively manage the stations.
- **Source Routing Group**: Collects the source routing information potentially present in any Token-Ring data packet.

The 8239 Model 1 provides full support for these groups.

Configuring the 8239 Model 1 to Support RMON

In order to collect RMON information, the RMON group must be enabled. The 8239 Model 1 factory setting enables all of the RMON groups. Once enabled, the status of the groups and tables is as follows.

- MAC-layer Statistics are set up
- Promiscuous Statistics are set up
- History: Two history control tables are set up per interface
  - Short-term poll with an interval of every 30 seconds

  - Long-term poll with an interval of every 30 minutes
- Host: One control table, one hosttable, and one hosttimetable per interface are set up
- HostTopN is not set up to be updated
- Matrix: One per interface is set up
- Event: Two events are set up
  - Internal log event (log only)
  - MIB II event (log and trap to the entry in the trap community)
- Alarm: no alarms are set up
- Filter: no filters are set up
- Packet Capture: packet capture is not active until a filter is set up
- Ring Station groups are active

To disable an individual RMON group, issue an SNMP Set request to the appropriate object in the 8239 MIB or issue the DISABLE RMON terminal interface command. The DISABLE RMON command can also be used to disable all of the RMON groups.

To determine which RMON groups are enabled, issue an SNMP Get request to the appropriate object in the 8239 MIB or issue the DISPLAY RMON GROUP_STATUS terminal interface command. When one or more RMON groups are enabled, RMON Mode is displayed by the DISPLAY MANAGMENT_INTERFACE terminal interface command; otherwise, DISABLED is displayed.

In order for source routing statistics to be accurate, the 8239 Model 1 must know the ring segment number. If there is an external RPS on the ring, then no action is required; otherwise, the 8239 Model 1 must be configured with the ring segment number. A ring number needs to be configured if the ring segment number displayed after issuing the DISPLAY MANAGMENT_INTERFACE command is 0. To configure the segment number, use one of these commands or MIBs:

- SET TR_SURROGATE SEGMENT_NUMBER (IBM TR Surrogate MIB)
- ENABLE TR_SURROGATE SURR_STATUS SURR_ADMIN (8239 MIB)

Note: If you want to enable RPS on the 8239 Model 1, refer to “Ring Parameter Server (RPS)” on page 8-26 for details.

Accessing RMON Information

To obtain RMON information, it is recommended that you use RMON Management Software that provides a graphical user interface, such as IBM's Nways Manager for AIX Remote Monitor or Nways Workgroup Remote Monitor for Windows NT.

The 8239 Model 1 also supports obtaining RMON information using the terminal interface. This method is especially useful if there is a connectivity problem to your RMON Management Software. The RMON-related terminal interface commands are:

```
CLEAR RMON
DISPLAY EVENT_SCRIPT
DISPLAY RMON ALARM_DATA
DISPLAY RMON CONTROL
DISPLAY RMON EVENT_DATA
```

DISPLAY RMON GROUP_STATUS
DISPLAY RMON HISTORY_ML_DATA
DISPLAY RMON HISTORY_P_DATA
DISPLAY RMON HOST_DATA
DISPLAY RMON LOG_DATA
DISPLAY RMON MATRIX_DATA
DISPLAY RMON RINGSTATION_DATA
DISPLAY RMON STATISTICS_DATA
DISPLAY RMON TOPN_HOSTS_DATA
DISPLAY TRAP_COMMUNITY
SET EVENT_SCRIPT
SET RMON ALARM
SET RMON EVENT
SET RMON HISTORY_CONTROL
SET RMON TOPN_HOSTS
SET TRAP_COMMUNITY

RMON 2

RMON 2 consists of the following MIBs:

- RMON 2 MIB (IETF RFC 2021)
- RMON MIB Protocol Ids (IETF RFC 2074)

RMON 2 decodes packets at layers 3 through 7 of the OSI model. An RMON 2 probe can monitor traffic on the basis of network-layer protocols and addresses, including the Internet Protocol (IP). This capability enables the probe to look beyond the LAN segments to which it is attached and to see traffic that goes across interconnect devices like routers.

The RMON 2 MIB is an extension of the original RMON MIB that contains a number of additional groups. These groups are:

- **Protocol Directory**: A master directory of all of the protocols that the probe can interpret.
- **Protocol Distribution**: Aggregate statistics on the amount of traffic generated by each protocol, per LAN segment.
- **Addressmap**: Matches each network address (Layer 3) to a specific MAC address and interface on an attached device and the physical address on this subnetwork.
- **Network-layer Host**: Statistics on the amount of traffic into and out of hosts based on network-layer addresses.
- **Network-layer Matrix**: Statistics on the amount of traffic between pairs of hosts (conversations) based on network-layer addresses.
- **Application-layer Host**: Statistics on the amount of traffic into and out of hosts based on application-layer addresses. The traffic broken down by protocols can be recognized by Protocol Directory.
- **Application-layer Matrix**: Statistics on the amount of traffic between pairs of hosts (conversations) based on application-layer addresses. The traffic broken down by protocols can be recognized by Protocol Directory.

- **User History Collection**: Periodically samples user-specified variables and logs the RMON 2 data based on user-defined parameters.
- **Probe Configuration**: Defines standard configuration parameters for an RMON/RMON 2 probe to provide remote capability of performing tasks that would normally require an out-of-band connection, such as a direct serial connection.
- **RMON Conformance**: Provides information regarding the status of support for the groups.

The 8239 Model 1 supports all of the RMON 2 groups with the following exceptions:

- Some of the Probe Configuration group items affect access to the RMON function in the 8239 Model 1, but they can also affect the availability of the hub or change characteristics of the hub used for accessing and managing the stack. Thus the following items are not supported by the RMON 2 MIB but similar function is available using the 8239 MIB or the 8239 Model 1 terminal interface.
  - For the Serial Configuration Table and the Serial Connection Table, use the following terminal interface commands:
    - DISPLAY TERMINAL
    - SET TERMINAL
  - Under the Probe Configuration group:

    probeDateTime DISPLAY CLOCK, REPLICATE_CLOCK, SET CLOCK

    probeResetControl RESET_HUB (you may want to issue SAVE first)

    probeDownloadFile LOAD OPERATIONAL_CODE

    probeDownloadTFTPServer LOAD OPERATIONAL_CODE

    probeDownloadAction LOAD OPERATIONAL_CODE
  - The NetWork Configuration Table is supported but the 8239 Model 1 supports only reading entries (SNMP Get requests), not writing entries (SNMP Set requests). Instead, issue an SNMP Set request to the appropriate object in the 8239 MIB or issue the SET IP ADDRESS terminal interface command.
- RMON Conformance group is not supported by the 8239 Model 1.

Configuring the 8239 Model 1 to Support RMON 2

The factory setting enables RMON 2. The following RMON 2 groups are automatically active:

- Address Table
- Protocol Distribution

To disable RMON 2, issue an SNMP Set request to the appropriate object in the IBM 8239 MIB or issue the command SET MANAGEMENT_INTERFACE RMON2_MODE NONE. After disabling RMON 2, you must save the configuration (using the SAVE command) and reset the 8239 Model 1 (using the RESET_HUB command) before the request will take effect.

To enable or disable the RMON 2 groups, it is recommended that you use RMON Management Software that provides a graphical user interface such as IBM's Nways Manager for AIX Remote Monitor or Nways Workgroup Remote Monitor for Windows NT.

RMON 2 groups cannot be enabled or disabled individually using the terminal interface. They can be disabled as a group by disabling all of the RMON groups. To disable all of the groups, issue an SNMP Set request to the appropriate object in the 8239 MIB or issue the ENABLE/DISABLE RMON ALL terminal interface command.

Accessing RMON 2 Information

To obtain RMON 2 information, it is recommended that you use RMON Management Software that provides a graphical user interface such as IBM's Nways Manager for AIX Remote Monitor or Nways Workgroup Remote Monitor for Windows NT.

RMON 2 information is not available using the terminal interface.

RMON Protocols

This section lists the protocols supported by operational code version 1.0 or later. It contains these subsections:

- Protocol overview
- Predefined protocols
- User-defined protocols

Protocol Overview: Each entry in the protocol directory table on a device represents a protocol that the device can decode and count. These protocols can be standard or custom.

The entries within the table are indexed by each data-link layer protocol: first, by MAC-layer protocol and then, by each level of encapsulated protocol. For example:

llc	Denotes the LLC (802.2) protocol
llc.ip	Denotes IP running over LLC protocol
llc.ip.udp	Denotes UDP running over IP over LLC
llc.ip.udp.snmp	Identifies the application-level protocol SNMP operating over LLC

The MAC-layer protocols consist of:

ether2	Ethernet II
llc	LLC (802.2) protocol
snap	Subnetwork access protocol
vsnap	Pseudo-protocol associated with snap
ianaAssigned	Those protocols that do not conform to the format of the other link-layer branches
anyLink	A wildcard protocol, identified by the prefix "*", that aggregates all link-layer protocols by their layer 2 encapsulated protocol. For example, if IPX is the layer 2 encapsulated protocol, the denotation is:

**.ipx ~ ether2.ipx + llc.ipx + snap.ipx + ianaAssigned.ipx*, where ~ indicates equivalence.

The anyLink protocol is enabled as a default for operational code version 1.0 or later.

Predefined Protocols: This section gives predefined protocols supported by operational code version 1.0 or later. Encapsulated protocols are listed alphabetically and the MAC-layer protocols over which they run are marked. For example, the 802.1-bridge protocol appears as both

```
*.802.1-bridge
llc.802.1-bridge
```

Table 8-1 (Page 1 of 3). Protocol Names

Protocols	Protocol Name
802.1-bridge	802.1D Bridge Spanning Tree
aarp	AppleTalk Address Resolution Protocol
adsp	AppleTalk Data Stream Protocol
aep	AppleTalk Echo Protocol
arp	Address Resolution Protocol
atalk	AppleTalk Datagram Delivery (short and long headers)
atp	AppleTalk Transaction Protocol
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
ccmail	Lotus cc-Mail
dec-diag	DEC Diagnostic
dns	Domain Name Service
drp	DECnet (Phase IV) Routing Protocol
ftp	File Transfer Protocol Control Port
ftp-data	File Transfer Protocol Data Port
gopher	Internet Document Search and Retrieval
icmp	Internet Control Message Protocol
idp	XNS Internet Datagram Protocol
igrp	Inter-Gateway Routing Protocol
ip	Internet Protocol
ipx	Internet Packet Exchange
nbp	AppleTalk Name Binding Protocol
lat	DECnet Local Area Transport
lavc	Local Area Vax Cluster
mop	DECnet Maintenance Operations Protocol
nbt_data	NetBIOS Datagram Support
nbt_name	NetBIOS Name Support
nbt_session	NetBIOS Session Support
netbeui	LAN Manager Netbeui

Table 8-1 (Page 2 of 3). Protocol Names	
Protocols	**Protocol Name**
netbios-3com	3Com NetBIOS
news	Network Window Service
nfs	Network File Service
nntp	Network News Transfer Protocol
notes	Lotus Notes
nov-bcast	Novell Broadcast
nov-diag	Novell Diagnostic
nov-echo	Novell Echo
nov-error	Novell Error-Handler
nov-ncp	Novell Netware Core Protocol
nov-netbios	Novell NetBIOS
nov-pep	Novell Packet Exchange Protocol
nov-rip	Novell Routing Information Protocol
nov-sap	Novell Service Advertising Protocol
nov-sec	Novell Security
nov-spx	Novell Sequenced Packet Exchange
nov-watchdog	Novell Watchdog
nsp	DECnet Network Services Protocol
ntp	Network Time Protocol
ospf	Open Shortest Path First
pop3	Post Office Protocol Version 3
printer	Printer
rcmd	Remote Command
rexec	Remote Process Execution
rlogin	Remote Login
router	Local Routing Processes (520/upd)
rtmp	AppleTalk Routing Table Maintenance Protocol
rwho	Remote Who
smb	Microsoft Server Message Block
smtp	Simple Mail Transfer Protocol
sna	Systems Network Architecture
snmp	Simple Network Management Protocol
snmptrap	Simple Network Management Protocol TRAPS
sunrpc	SUN Remote Procedure Call
tcp	Transmission Control Protocol
telnet	Network Virtual Terminal
tftp	Trivial File Transfer Protocol
udp	User Datagram Protocol

Table 8-1 (Page 3 of 3). Protocol Names	
Protocols	**Protocol Name**
varp	Banyan VINES Address Resolution Protocol
vecho	Banyan VINES Data Link Level Echo
vicp	Banyan VINES Internet Control Protocol
vip	Banyan VINES Internet Protocol
vipc	Banyan VINES InterProcess Communications
vipc-dgp	Banyan VINES Unreliable Datagram Protocol
vipc-rdp	Banyan VINES Reliable Datagram Protocol
vrtp	Banyan VINES Routing Update Protocol
vspp	Banyan VINES Sequenced Packet Protocol
www-http	World Wide Web HTTP
X	X Windows
xns-echo	XNS Echo
xns-error	XNS Error-Handler
xns-pep	XNS Packet Exchange Protocol
xns-rip	XNS Routing Information Protocol
xns-spp	XNS Sequenced Packet Protocol
zip	Zone Information Protocol

Table 8-2 (Page 1 of 5). Predefined Protocols					
MAC-Layer Protocol					
***.**	**llc.**	**snap.**	**vsnap_ ether2.**	**ianaAs- signed.**	**Encapsulated Protocols**
√	√				802.1-bridge
√		√			aarp
√		√			arp
√		√	√		atalk
√		√	√		atalk.adsp
√		√	√		atalk.aep
√		√	√		atalk.atp
√		√	√		atalk.atp.zip
√		√	√		atalk.nbp
√		√	√		atalk.rtmp
√		√	√		atalk.snmp
√		√	√		atalk.snmptrap
√		√	√		atalk.zip
√		√			dec-diag
√		√			drp
√		√			drp.nsp
√		√			idp

Table 8-2 (Page 2 of 5). Predefined Protocols

MAC-Layer Protocol					Encapsulated Protocols
*.	llc.	snap.	vsnap_ ether2.	ianaAs- signed.	
√		√			idp.xns-echo
√		√			idp.xns-error
√		√			idp.xns-pep
√		√			idp.xns-rip
√		√			ipd.xns-spp
√	√	√			ip
√	√	√			ip.icmp
√	√	√			ip.igrp
√	√	√			ip.ip
√	√	√			ip.ip.icmp
√	√	√			ip.ip.igrp
√	√	√			ip.ip.opsf
√	√	√			ip.ip.tcp
√	√	√			ip.ip.tcp.ccmail
√	√	√			ip.ip.tcp.dns
√	√	√			ip.ip.tcp.ftp
√	√	√			ip.ip.tcp.ftp-data
√	√	√			ip.ip.tcp.gopher
√	√	√			ip.ip.tcp.nbt_data
√	√	√			ip.ip.tcp.nbt_data.smb
√	√	√			ip.ip.tcp.nbt_name
√	√	√			ip.ip.tcp.nbt_session
√	√	√			ip.ip.tcp.nbt_session.smb
√	√	√			ip.ip.tcp.news
√	√	√			ip.ip.tcp.nntp
√	√	√			ip.ip.tcp.notes
√	√	√			ip.ip.tcp.pop3
√	√	√			ip.ip.tcp.printer
√	√	√			ip.ip.tcp.rcmd
√	√	√			ip.ip.tcp.rexec
√	√	√			ip.ip.tcp.rlogin
√	√	√			ip.ip.tcp.smtp
√	√	√			ip.ip.tcp.snmp
√	√	√			ip.ip.tcp.snmptrap
√	√	√			ip.ip.tcp.telnet
√	√	√			ip.ip.tcp.www-http
√	√	√			ip.ip.tcp.X

Table 8-2 (Page 3 of 5). Predefined Protocols

MAC-Layer Protocol					Encapsulated Protocols
***.**	**llc.**	**snap.**	**vsnap_ ether2.**	**ianaAs- signed.**	
√	√	√			ip.ip.udp
√	√	√			ip.ip.udp.bootpc
√	√	√			ip.ip.udp.bootps
√	√	√			ip.ip.udp.ccmail
√	√	√			ip.ip.udp.dns
√	√	√			ip.ip.udp.nbt_data
√	√	√			ip.ip.udp.nbt_data.smp
√	√	√			ip.ip.udp.nbt_name
√	√	√			ip.ip.udp.nbt_session
√	√	√			ip.ip.udp.nbt_session.smp
√	√	√			ip.ip.udp.notes
√	√	√			ip.ip.udp.ntp
√	√	√			ip.ip.udp.printer
√	√	√			ip.ip.udp.router
√	√	√			ip.ip.udp.rwho
√	√	√			ip.ip.udp.snmp
√	√	√			ip.ip.udp.snmptrap
√	√	√			ip.ip.udp.sunrpc
√	√	√			ip.ip.udp.sunrpc.nfs
√	√	√			ip.ip.udp.tftp
√	√	√			ip.ip.udp.X
√	√	√			ip.ospf
√	√	√			ip.tcp
√	√	√			ip.tcp.ccmail
√	√	√			ip.tcp.dns
√	√	√			ip.tcp.ftp
√	√	√			ip.tcp.ftp-data
√	√	√			ip.tcp.gopher
√	√	√			ip.tcp.nbt_data
√	√	√			ip.tcp.nbt_data.smb
√	√	√			ip.tcp.nbt_name
√	√	√			ip.tcp.nbt_session
√	√	√			ip.tcp.nbt_session.smb
√	√	√			ip.tcp.news
√	√	√			ip.tcp.nntp
√	√	√			ip.tcp.notes
√	√	√			ip.tcp.pop3

Table 8-2 (Page 4 of 5). Predefined Protocols

MAC-Layer Protocol					Encapsulated Protocols
***.**	**llc.**	**snap.**	**vsnap_ ether2.**	**ianaAs- signed.**	
√	√	√			ip.tcp.printer
√	√	√			ip.tcp.rcmd
√	√	√			ip.tcp.rexec
√	√	√			ip.tcp.rlogin
√	√	√			ip.tcp.smtp
√	√	√			ip.tcp.snmp
√	√	√			ip.tcp.snmptrap
√	√	√			ip.tcp.telnet
√	√	√			ip.tcp.www-http
√	√	√			ip.tcp.X
√	√	√			ip.udp
√	√	√			ip.udp.bootpc
√	√	√			ip.udp.bootps
√	√	√			ip.udp.ccmail
√	√	√			ip.udp.dns
√	√	√			ip.udp.nbt_data
√	√	√			ip.udp.nbt_data.smb
√	√	√			ip.udp.nbt_name
√	√	√			ip.udp.nbt_session
√	√	√			ip.udp.nbt_session.smb
√	√	√			ip.udp.notes
√	√	√			ip.udp.ntp
√	√	√			ip.udp.printer
√	√	√			ip.udp.router
√	√	√			ip.udp.rwho
√	√	√			ip.udp.snmp
√	√	√			ip.udp.snmptrap
√	√	√			ip.udp.sunrpc
√	√	√			ip.udp.sunrpc.nfs
√	√	√			ip.udp.tftp
√	√	√			ip.udp.X
√	√	√		√	ipx
√	√	√		√	ipx.nov-echo
√	√	√		√	ipx.nov-error
√	√	√		√	ipx.nov-netbios
√	√	√		√	ipx.nov-netbios.notes
√	√	√		√	ipx.nov-netbios.smb

Table 8-2 (Page 5 of 5). Predefined Protocols

MAC-Layer Protocol					Encapsulated Protocols
***.**	**llc.**	**snap.**	**vsnap_ ether2.**	**ianaAs- signed.**	
√	√	√		√	ipx.nov-pep
√	√	√		√	ipx.nov-pep.nov-bcast
√	√	√		√	ipx.nov-pep.nov-diag
√	√	√		√	ipx.nov-pep.nov-netbios
√	√	√		√	ipx.nov-pep.nov-netbios.notes
√	√	√		√	ipx.nov-pep.nov-netbios.smb
√	√	√		√	ipx.nov-pep.nov-rip
√	√	√		√	ipx.nov-pep.nov-sap
√	√	√		√	ipx.nov-pep.nov-sap.notes
√	√	√		√	ipx.nov-pep.nov-sap.nov-ncp
√	√	√		√	ipx.nov-pep.nov-sec
√	√	√		√	ipx.nov-pep.nov-watchdog
√	√	√		√	ipx.nov-pep.smb
√	√	√		√	ipx.nov-pep.snmp
√	√	√		√	ipx.nov-pep.snmptrap
√	√	√		√	ipx.nov-rip
√	√	√		√	ipx.nov-spx
√		√			lat
√		√			lavc
√		√			mop
√	√				netbeui
√	√				netbeui.notes
√	√				netbeui.smb
√					netbios-3com
√	√				sna
√	√	√			vecho
√	√*	√			vip
√	√*	√			vip.varp
√	√*	√			vip.vicp
√	√*	√			vip.vipc
√	√*	√			vip.vipc.vipc-dgp
√	√*	√			vip.vipc.vipc-rdp
√	√*	√			vip.vrtp
√	√*	√			vip.vspp

Note: * These protocols running over LLC are displayed as *llc.vtr.vecho* and so on, where *vtr* is an additional protocol layer.

User-Defined Protocols: If you are using customized protocols or protocol encapsulations on your network, you may want to add these to your protocol directory using a management application such as IBM Nways Manager or IBM Nways Workgroup Remote Monitor.

With operational code version 1.0 or later installed on the 8239, you can specify at least 64 wildcard protocols or 256 non-wildcard protocols; see “Protocol Overview” on page 8-10 for a description of the anyLink or wildcard protocol.

Operational code version 1.0 or later supports a number of extensible protocols, as shown in Table 8-3, with the following exceptions:

- ipx is not extensible by either values 0 or 17
- llc is not extensible by odd-numbered children
- nov-sap, nsp, sunrpc, vip, vipc, and vsnap are not extensible

The maxchildren value shows the total number of child protocols that may be defined. This value is calculated irrespective of the encapsulation used. For example, *ether2.ip.upd* and *llc.ip.udp* would be counted as one child only.

Table 8-3. Extensible Protocols and maxChildren Values

Protocol	maxChildren		
	Total	**Pre-Defined**	**User-Defined**
atalk	16	9	7
idp	8	5	3
ip	256	7	249
ip.ip	16	7	9
ipx	256	5	249*
llc	256	8	120†
nov-pep	16	11	5
nov-spx	16	0	16
snap	32	14	18
tcp	64	22	42
udp	64	17	47
vipc-dgp	4	0	4
vipc-rdp	4	0	4
vspp	4	0	4
xns-pep	4	0	4
xns-spp	4	0	4

Notes:

* ipx is not extensible by either values 0 or 17

† llc is not extensible by odd-numbered children

ECAM

ECAM supports Protocol Distribution and Address Translation. Protocol Distribution provides information on what network protocols are being used, such as what amount of your network traffic consists of which protocols, which stations have conversations with each other using which protocols, and so on. Address Translation provides a mapping between MAC addresses and network addresses (IP addresses or host names). Address Translation in ECAM also provides the ability to identify duplicate addresses.

Configuring the 8239 Model 1 to Support ECAM

The factory setting disables ECAM for the 8239 Model 1. The following ECAM groups are automatically active:

- Address Table
- Protocol Distribution

To enable ECAM, issue an SNMP Set request to the appropriate object in the 8239 MIB or issue the command SET MANAGEMENT_INTERFACE RMON2_MODE ECAM. After enabling ECAM, you must save the configuration (using the SAVE command) and reset the 8239 Model 1 (using the RESET_HUB command) before the request will take effect. Once the 8239 Model 1 is operational with ECAM enabled, ECAM is not active (running) until this is requested via SNMP.

To activate ECAM and enable or disable the ECAM groups, it is recommended that you use RMON Management Software that provides a graphical user interface such as IBM's Nways Manager for AIX Remote Monitor or Nways Workgroup Remote Monitor for Windows NT. Follow the instructions provided for SmartAgent dialogs or configuration. The TFTP Server Address is not needed to start or stop ECAM on the 8239 Model 1.

ECAM groups cannot be enabled or disabled individually using the terminal interface. They can be disabled as a group by disabling all of the RMON groups. To disable all of the groups, issue an SNMP Set request to the appropriate object in the IBM 8239 MIB or issue the ENABLE/DISABLE RMON ALL terminal interface command.

Accessing ECAM Information

To obtain ECAM information, it is recommended that you use RMON Management Software that provides a graphical user interface such as IBM’s Nways Manager for AIX Remote Monitor or Nways Workgroup Remote Monitor for Windows NT.

ECAM information is not available using the terminal interface.

RMON Tables

When an RMON table becomes full, new entries will not be added to the table. The RMON table must be deleted or cleared in order for the table to be automatically rebuilt based on current traffic data. RMON tables can be cleared through SNMP or the terminal interface. RMON 2 tables can only be cleared using SNMP.

Depending on your network configuration and network traffic characteristics, you may want to periodically delete or clear the RMON and RMON 2 tables. RMON events and alarms can be used to indicate when a table is full.

When deleting large RMON or RMON 2 tables, in-band connectivity to the 8239 Model 1 Management Interface may be lost temporarily. However, in-band connectivity to the Management Interface automatically resumes once the table deletion processing is completed. Other hub operations are not affected.

Table 8-4, Table 8-5 on page 8-21, and Table 8-6 on page 8-21 show the maximum number of entries for each RMON, RMON 2, and ECAM table.

Table 8-4. Maximum Number of Entries in Each RMON Table	
Alarm Entries	60
Buffer Control Entries	16
Capture Buffer Packets	8 000
Capture Buffer Total Octets	1 048 576
Channel Entries	40
Event Table	150
Filter Entries	60
History Control Table	10
Host Data Table	30 000
Host Top N Control Table	10
Log Table	2 800
Mac-Layer Statistics Table	1
Matrix Data Table	18 000
Promiscuous Statistics Table	1
Ring Station Table	300
Source Routing Statistics Table	1

Table 8-5. Maximum Number of Entries in Each RMON 2 Table	
addressMapControlTable	3
addressMapTable	40 000
alHostTable	10 000
alMatrixDSTable	40 000
alMatrixSDTable	40 000
alMatrixTopNControlTable	4
alMatrixTopNTable	25 000
hlMatrixControlTable	3
hlMatrixDSTable	40 000
hlMatrixSDTable	40 000
hlMatrixTopNControlTable	4
hlMatrixTOPNTable	25 000
netConfigTable	1
nlHostControlTable	3
nlHostTable	10 000
protocolDirTable	1 300
protocolDistControlTable	1
protocolDistTable	1 000
userHistoryControlTable	10
userHistoryObjectTable	16 per bucket
trapDestTable	300
userHistoryTable	1 164

Table 8-6. Maximum Number of Entries in Each ECAM Table	
atTable	1 024
hlHostTable	200
hlMatrixTable	256
hlStatsTable	2 048
protocolDirectoryTable	256

IBM Token-Ring Surrogate MIB and Surrogate Trap MIB

The 8239 Model 1 contains a Surrogate Agent that is defined by the following MIBs:

- IBM Surrogate MIB
- IBM Surrogate Trap MIB

The Surrogate Agent consists of the Surrogate Group and the following server functions:

- CRS
- REM

- RPS

CRS, REM, and RPS allow active media management of Token-Ring networks. REM analyzes MAC errors locally, providing early detection and assistance in locating the problem source. CRS provides accurate displays of stations and their order on the ring. RPS provides operational parameters to Token-Ring stations so that they can be centrally managed.

The IBM Surrogate Trap MIB contains traps that the server functions send to provide real-time information about occurrences on the network to an SNMP Management Application such as IBM's Nways Campus Manager LAN for AIX.

Surrogate Group

The Surrogate Group contains information regarding the administrative and operational status of the CRS, REM, and RPS servers. It also provides the following information:

- The MAC address being used by the Surrogate Agent
- The ring segment number
- Ring utilization

Configuring the 8239 Model 1 to Support the Surrogate Group

To use any of the Surrogate Agent functions, you must enable the Surrogate Group. The factory setting for the Surrogate Group is disabled. To enable the Surrogate Group, issue an SNMP Set request to the appropriate MIB object in the IBM 8239 MIB or use either one of the following terminal interface commands:

- ENABLE TR_SURROGATE SURR_STATUS SURR_ADMIN
- SET MANAGEMENT_INTERFACE SURROGATE_GROUP ENABLE

Although the Surrogate Group administrative state is not part of the Surrogate MIB, this state allows you to easily activate or deactivate all of the Surrogate server functions. It also allows you to obtain ring utilization information and update the ring segment number without having any of the Surrogate server functions operational.

Accessing Surrogate Group Information

The Surrogate Group information can be obtained using the following methods.

- SNMP
  - Using the IBM Token Ring Surrogate MIB, surrogateStatusTable. For this MIB, the ibmTokenRing object identifier (OID) is 1.3.6.1.4.1.2.5 and the tokenringSurrogate OID is ibmTokenRing.1.
  - For the Surrogate Group administrative state, issue an SNMP Get request for the appropriate object in the 8239 MIB
- The terminal interface, using the following commands:
  - DISPLAY TR_SURROGATE SURR_STATUS

    This command displays all of the information associated with the surrogateStatusTable and also provides the administrative state of the Surrogate Group.
  - DISPLAY MANAGEMENT_INTERFACE

    This command provides the administrative state of the Surrogate Group, that is, whether the Surrogate Group is enabled or disabled. It also

identifies the ring segment number that is currently being used. This value can differ from the ring segment number displayed with the DISPLAY TR_SURROGATE command, as described in detail below.

– SET TR_SURROGATE SEGMENT_NUMBER

  This command configures the Surrogate Agent with a ring segment.

The MAC address used by the Surrogate Agent is the same MAC address that is associated with the Management Interface.

The ring segment number is the number that is to be used when the 8239 Model 1 is the RPS. When the 8239 Model 1 RPS function is not enabled and there is no external RPS on the ring, then the ring segment number should be set so that the 8239's RMON agent can update its source-routing statistics properly.

The ring segment number obtained by issuing the DISPLAY TR_SURROGATE SURR_STATUS command or an SNMP Get Request of the surrogateStatusTable in the Surrogate MIB is always the ring segment number that you configure for the 8239 Model 1 using the SET TR_SURROGATE SEGMENT_NUMBER command or the SNMP Set Request to the surrogateStatusTable.

The ring segment number that is displayed using the DISPLAY MANAGEMENT_INTERFACE command or an SNMP Get request to the appropriate object in the 8239 MIB is the active ring number known for the ring. The 8239 Model 1's configured ring number and the active ring number can be different if there is an external RPS on the ring that is using a different ring number from that configured on the 8239.

The ring utilization displayed using the DISPLAY TR_SURROGATE SURR_STATUS command is a percentage of the calculated ring utilization with a range from 0 to 100. When it is obtained via SNMP, it is a percentage of the calculated ring utilization in tenths of a percent with a range from 0 to 1000.

The administrative state of the server functions indicate whether or not you want the servers to be active. The operational state of the server functions indicate whether or not the servers are active.

Configuration Report Server (CRS)

CRS accumulates information by MAC address about what stations are on the ring, handles requests to set and display ring-station information, and removes stations from the ring on request. CRS can also provide real-time information when the ring segment topology changes.

CRS provides these functions:

- Allows active management of Token-Ring networks, gathering station information, and setting station parameters
- Provides an accurate display of all station MAC addresses on the ring being monitored and their order on the ring for generating network topology
- Reports ring topology changes

Configuring the 8239 Model 1 to Support CRS

You must administratively enable both the Surrogate and CRS functions to use CRS.

- To enable CRS, issue an SNMP Set request to the appropriate MIB object in the IBM TR Surrogate MIB or issue the ENABLE TR_SURROGATE SURR_STATUS CRS_ADMIN terminal interface command.
- To enable the Surrogate Group, see “Configuring for the Surrogate Agent” on page 4-8.

Part of the CRS function is to report ring topology changes by sending a trap. The factory setting for sending CRS traps is enabled. To get the CRS traps sent to an IP station, set up an entry in the 8239 Model 1's trap community table by issuing an SNMP Set request to the appropriate object in the 8239 MIB or issue the SET TRAP_COMMUNITY TR_SURROGATE terminal interface command.

To disable CRS from generating traps, issue an SNMP Set request to the appropriate object in the IBM TR Surrogate MIB or issue the DISABLE TR_SURROGATE CRS_TRAPS terminal interface command.

Accessing CRS Information

The CRS group is formed by the CRS Status Table and the CRS Ring Station Table. Both of these tables can be accessed via SNMP using the IBM TR Surrogate MIB or by issuing the following terminal interface commands:

- DISPLAY TR_SURROGATE CRS_STATUS
- DISPLAY TR_SURROGATE CRS_STATION
- SET TR_SURROGATE CRS_STATION

When the CRS surrogate agent on the 8239 Model 1 is active, it sends CRS Request MAC frames to all stations participating in the token-ring Neighbor Notification Process every 10 minutes and after NAUN changes occur. If a station does not respond to the CRS Request frame, the 8239 sends out the CRS Request MAC frames every minute; if this situation occurs, the DISPLAY TR_SURROGATE CRS_STATION ALL command identifies the MAC address that did not respond so that you can take further action.

Ring Error Monitor (REM)

REM provides the following functions:

- Observes collects, and analyzes hard and soft error conditions on the ring
- Assists in fault isolation and correction

Configuring the 8239 Model 1 to Support REM

To use REM, you must administratively enable both the REM and Surrogate functions.

- To enable REM, issue an SNMP Set request to the appropriate MIB object in the IBM TR Surrogate MIB or issue the ENABLE TR_SURROGATE SURR_STATUS REM_ADMIN terminal interface command.
- To enable the Surrogate Group, refer to “Configuring for the Surrogate Agent” on page 4-8.

REM reports error conditions present on the ring and, when configured, can provide early warning that excessive errors may exist by sending traps. The remGenTrapFlag must be enabled for any traps to be sent by REM. In addition to the remGenTrapFlag, there are individual flag settings for sending out various traps associated with the data that REM is collecting and analyzing. These individual traps are:

- remWeightExceeded
- remPreWeightExceeded
- remNonIsoThresholdExceeded
- remReceiveCongestion
- remForwardFrames
- remRingLineErrors
- remRingInternalErrors
- remRingBurstErrors
- remRingACErrors
- remRingABortXmitted
- remRingLostFrames
- remRingReceiverCongestion
- remRingFrameCopied
- remRingFrequencyError
- remRingTokenError
- remAutoLineErrors
- remAutoInternalErrors
- remAutoBurstErrors
- remAutoACErrors
- remAutoABortXmitted
- remAutoLostFrames
- remAutoReceiverCongestion
- remAutoFrameCopied
- remAutoFrequencyError
- remAutoTokenError

The factory setting enables the sending of REM traps. To send the REM traps to an IP station, set up an entry in the 8239 Model 1's trap community table by issuing an SNMP Set request to the appropriate object in the IBM 8239 MIB or issue the SET TRAP_COMMUNITY TR_SURROGATE terminal interface command.

To disable REM from generating traps, issue an SNMP Set request to the appropriate object in the IBM TR Surrogate MIB or issue the DISABLE TR_SURROGATE REM_TRAPS terminal interface command. The factory settings disable the individual REM flags (prefixed by "remRing" and "remAuto"). To enable the individual REM traps, issue an SNMP Set request to the appropriate object in the IBM TR Surrogate MIB or issue one of the following terminal interface commands:

- To enable all flags, use ENABLE TR_SURROGATE REM_STATUS ALL_FLAGS
- To enable individual REM flags, use ENABLE TR_SURROGATE REM_STATUS, specifying the appropriate keyword for the desired flag

Be aware of the following consequences when enabling any of the REM individual traps:

- Enabling any of the ring-intensive flags may generate excessive soft error traps. Enable these flags only if you want to know each time a soft error MAC frame has a value greater than zero for the associated counter. From a given soft error MAC frame, a separate trap will be generated for every counter that is greater than zero in that frame.
- If any of the auto-intensive flags are enabled, a soft error trap is generated only when the counter in the soft error frame is greater than zero and the station is in a pre-weight or weight-exceeded condition.

Under normal conditions, it is useful to enable the following flags:

- remGenTrapFlag
- remWeightExceeded
- remPreWeightExceeded
- remNonIsoThresholdExceeded

When unexpected network problems occur, additional REM flags can be enabled to help analyze and isolate the problems.

Note: Traps reporting beaconing conditions on the network will be sent as long as remGenTrapFlag is enabled. Be aware that since the 8239 performs beacon recovery and may temporarily wrap ports including the Management Interface to isolate the fault, the 8239 Model 1 REM function may not be aware of all beacon frames that occur on the ring.

Accessing REM Information

The following tables are part of REM:

- Status Table
- Isolating Table
- Non-Isolating Threshold Exceeded Trap Table
- Soft Error Trap Table
- Total Soft Error Trap Table
- Last Received Soft Error Trap Table
- Beacon Data Trap Table
- Error MAC Frame Trap Table

The information in the above tables can be accessed via SNMP using the IBM TR Surrogate MIB or by issuing the following terminal interface commands:

- CLEAR TR_SURROGATE_REM_SOFT_ERROR
- DISPLAY TR_SURROGATE REM_ERROR_MAC_FRAME
- DISPLAY TR_SURROGATE REM_ISOLATING
- DISPLAY TR_SURROGATE REM_LAST_BEACON
- DISPLAY TR_SURROGATE REM_LAST_SOFT_ERROR
- DISPLAY TR_SURROGATE REM_NONISO_THRESHOLD_EXCD
- DISPLAY TR_SURROGATE REM_STATUS
- DISPLAY TR_SURROGATE REM_TOTAL_NONISO_SOFT_ERROR

Ring Parameter Server (RPS)

RPS is a Token-Ring media-management function that resides on rings where station operational parameters need to be centrally managed. RPS provides these functions:

- It is the target of the Request Initialization MAC frames that are sent by stations when they insert into the ring. This arrangement allows a station to send the

frame to a known address on the local segment without having to broadcast it to other rings. The RPS can then inform a network management application that a new station is present on the ring.

- It makes parameters, such as the ring segment number and ring station soft error report timer value, available to all ring stations on the ring. This availability guarantees that these values are the same for all stations on the ring.

Configuring the 8239 Model 1 to Support RPS

To use RPS, you must administratively enable both the Surrogate and RPS functions and configure the 8239 Model 1 with a valid ring segment number. The factory setting disables the Surrogate and RPS functions and there is no ring segment number. To make the RPS operational, follow these steps:

- To configure the ring segment number, issue an SNMP Set request to the appropriate object in the IBM TR Surrogate MIB or issue the SET TR_SURROGATE SEGMENT_NUMBER terminal interface command.
- To enable RPS, issue an SNMP Set request to the appropriate MIB object in the IBM TR Surrogate MIB or issue the ENABLE TR_SURROGATE SURR_STATUS RPS_ADMIN terminal interface command.
- To enable the Surrogate Group, refer to “Configuring for the Surrogate Agent” on page 4-8.

Note that the 8239 Model 1 RPS will not become active if either of the following conditions exists:

- A valid ring number has not been configured.
- There is another RPS already on the ring that is using a different ring segment number from that configured for the 8239 Model 1.

If another RPS is on the ring and that RPS is using the same ring segment number as that configured on the 8239 Model 1, then the Model 1’s RPS will also be active.

A portion of the RPS function is to report when stations insert into the ring by sending a trap. The factory setting for sending RPS traps is enabled. To send the RPS traps to an IP station, set up an entry in the 8239 Model 1’s trap community table by issuing an SNMP Set request to the appropriate object in the 8239 MIB or issue the SET TRAP_COMMUNITY TR_SURROGATE terminal interface command.

To disable RPS from generating traps, issue an SNMP Set request to the appropriate object in the 8239 MIB or issue any of the following terminal interface commands:

- DISABLE TR_SURROGATE RPS_TRAPS
- SET MANAGEMENT_INTERFACE RPS_TRAPS DISABLE

Accessing RPS Information

RPS contains the RPS Status Table, which consists of information about the last station that inserted into the ring. The RPS Status Table can be accessed:

- Through SNMP using the IBM TR Surrogate MIB
- By issuing the DISPLAY TR_SURROGATE RPS_STATUS terminal interface command.

The flag to indicate whether or not RPS traps should be generated is not part of the IBM TR Surrogate MIB but is part of the 8239 MIB. This flag can be accessed by an SNMP request to the appropriate object in the 8239 MIB or by issuing one of the following terminal interface commands:

- DISPLAY MANAGEMENT_INTERFACE
- DISPLAY TR_SURROGATE RPS_STATUS
- ENABLE/DISABLE TR_SURROGATE RPS_TRAPS
- SET MANAGEMENT_INTERFACE RPS_TRAPS ENABLE/DISABLE

Chapter 9. Planning Charts

8239 Cabling Chart

Identification

Check the appropriate box:

Ring Data Rate □ 4 Mbps □ 16 Mbps

Physical location:

Building Number _____ Unit Number _____
Wiring Closet/Room ____ Ring Number _____
Rack Number ____ MAC Address _____

Ring Connection for Optional RI/RO Module

	RI	RO
Connect to		
Device		

Token-Ring Port Connections

	1	2	3	4	5	6	7	8
Connect to								
Device								

	9	10	11	12	13	14	15	16
Connect to								
Device								

Additional Ports with Optional 16-Port Expansion Adapter

	17	18	19	20	21	22	23	24
Connect to								
Device								

	25	26	27	28	29	30	31	32
Connect to								
Device								

8239 SNMP Agent Configuration Parameters Worksheet

Parameter Name	Description	Your Data
IP Group Values		
IP Address	Address of 8239 SNMP agent	
IP Subnet Mask	8239 assigned subnet mask	
Default Gateway	8239-assigned default gateway	
MIB-II System Parameters		
System Description	Description of the 8239	
System Contact	Defines a contact name and telephone number	
System Name	Defines a name for the 8239	
System Location	Defines the location of the 8239	
Community Access (up to 20)		
Community Name	Community name up to any 128 characters with no spaces	
Access Level	Access Level for this community string	
Community Access Control (up to 20)		
Community Name	Community name up to any 128 characters with no spaces	
IP Address	IP address of the manager within the community	

Parameter Name	Description	Your Data
IP Mask	Mask to be applied (using logical AND) to the requesting manager's IP address before comparison with the communityAccessControl-IPAddress. If the result matches, the address is authenticated.	
Trap Community Specification (up to 30)		
IP Address	IP address of SNMP manager to receive alerts.	
Trap Community String	Community name up to any 128 characters with no spaces	
Trap Type All	If set to *enable*, the 8239 sends this type of alert to the configured trap communities. If set to *disable*, no alerts are sent.	
Trap Type Private	If set to *enable*, the 8239 sends this type of alert to the configured trap communities. If set to *disable*, no alerts are sent.	
Trap Type RMON	If set to *enable*, the 8239 sends this type of alert to the configured trap communities. If set to *disable*, no alerts are sent.	
Trap Type Surrogate	If set to *enable*, the 8239 sends this type of alert to the configured trap communities. If set to *disable*, no alerts are sent.	
Trap Type MIB2	If set to *enable*, the 8239 sends this type of alert to the configured trap communities. If set to *disable*, no alerts are sent.	
8239 Terminal Interface Program (EIA 232 Interface)		

Parameter Name	Description	Your Data
Login Name	Login name to allow access to the terminal interface. Using **admin** with no password is the default.	
Login Password	Password to allow access to the terminal interface	

Appendix A. Warranty Information

This appendix contains these warranty statements:

- Customer Carry-In Exchange via Mail-In
- Statement of Limited Warranty

Customer Carry-In Exchange via Mail-In

Supplemental Information

Terms and Conditions

Warranty Period: One Year

Warranty Service: Customer Carry-In Exchange (CCE) via Mail-In. Monday through Friday, 8:00 A.M. to 5:00 P.M., excluding holidays.

If warranty terms, conditions, or service is required, the customer should call IBM. In the U.S., call IBM at 800-772-2227; in Canada, call 1-800-IBM-SERV (1-800-426-7378). The HelpCenter will assist the user with problem determination and will initiate shipment of a replacement unit, if needed, to the customer's location by express delivery. For calls received by 5:00 P.M. customer's time, in most cases, the replacement unit will arrive within two business days. The replacement unit becomes the property of the customer in exchange for the failed unit, which becomes the property of IBM. The customer needs to pack the failed unit into the shipping carton that contained the replacement unit. IBM will then arrange for its collection.

Transportation charges, both ways, will be paid by IBM.

Failure to use the carton in which the replacement unit was received could result in charges incurred by the customer for damage to the failed unit during shipment. These terms cover most continental U.S. locations (cities defined by FedEx as H1 or H2 designated locations). Contact 800-463-3339 (GO-FEDEX) for specific delivery schedule information.

Alternate Service: IBM On-Site Repair (IOR)

The warranty upgrade provides IOR, Monday through Friday, 8:00 A.M. to 5:00 P.M., (excluding holidays), with next business-day response.

Maintenance Service: IBM On-Site Repair (IOR) post-warranty maintenance service is available under IBM Customer Agreement.

The post-warranty offering provides IOR, Monday through Friday, 8:00 A.M. to 5:00 P.M., (excluding holidays), with next business-day response.

If warranty upgrade or post-warranty maintenance service is required, the customer should call IBM at 800-IBM-SERV (800-426-7378). IBM will assist the user with problem determination and will dispatch on-site service personnel to the customer's location , if needed, with the required replacement part. For calls received by 5:00

P.M. customer's time, in most cases, a service representative will arrive next business day.

Statement of Limited Warranty

International Business Machines Corporation Armonk, New York, 10504

The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you originally purchase for your use, and not for resale, from IBM or your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. If you have any questions, contact IBM or your reseller.

Machine:	8239
Warranty Period*:	1 year

**Contact your place of purchase for warranty service information.*

Production Status

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

The IBM Warranty for Machines

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

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

For IBM or your reseller to provide warranty service for a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many of these transactions involve the removal of parts and their return to IBM. You represent that all removed parts are genuine and unaltered. A part that replaces a removed part will assume the warranty service status of the replaced part.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair it or replace it with one that is at least functionally equivalent, without charge. The replacement may not be new, but will be in good working order. If IBM or your reseller is unable to repair or replace the Machine, you may return it to your place of purchase and your money will be refunded.

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

and this Statement to that user. However, for Machines which have a life-time warranty, this warranty is not transferable.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at **1-800-772-2227**. In Canada, call IBM at **1-800-IBM-SERV (1-800-426-7378)**. You may be required to present proof of purchase.

IBM or your reseller will provide certain types of repair and exchange service, either at your location or at IBM's or your reseller's service center, to restore a Machine to good working order.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item. Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service. You also agree to ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange.

You agree to:

1. obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
2. where applicable, before service is provided —
   a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
   b. secure all programs, data, and funds contained in a Machine, and
   c. inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Extent of Warranty

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

The warranties may be voided by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, removal or alteration of Machine or parts identification labels, or failure caused by a product for which IBM is not responsible.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN

THAT EVENT SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Limitations of Liability

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

1. damages for bodily injury (including death) and damage to real property and tangible personal property; and
2. the amount of any other actual direct damages or loss, up to the greater of U.S. $100,000 or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR LOSSES OR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE); 2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

Appendix B. Wrap Point References

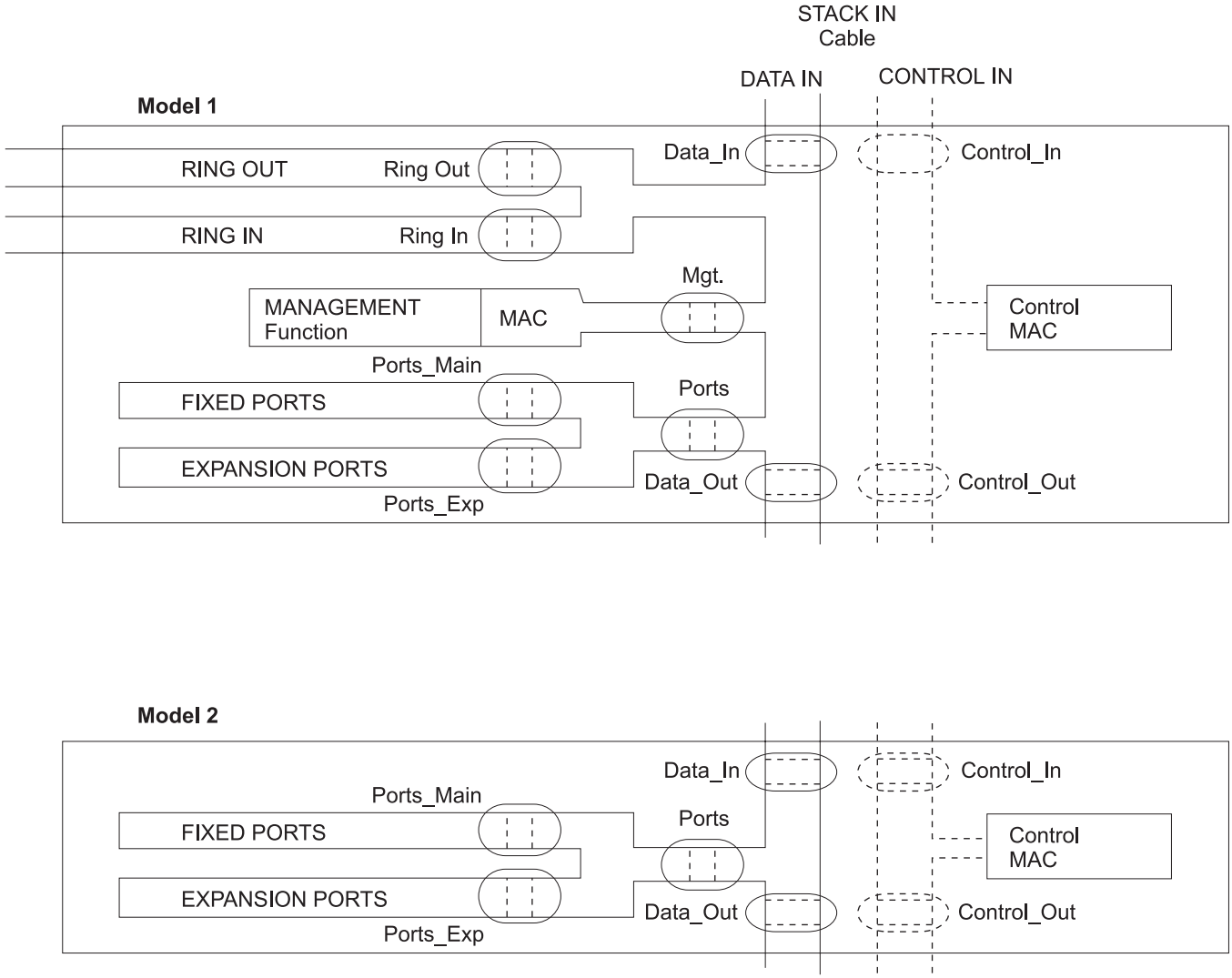

Figure B-1. Wrap Points for the Model 1 and Model 2

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to terms that have a related, but not synonymous, meaning.

A

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. A method for mapping network layer addresses onto media-specific addresses. See also *Address Resolution Protocol (ARP).*

Address Resolution Protocol (ARP). In the internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting LAN, such as Ethernet or token ring.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

ARP. Address Resolution Protocol.

ARP cache. A local cache used to translate IP addresses into physical addresses.

B

beacon. A frame sent by an adapter indicating a serious ring problem, such as a broken cable.

beacon recovery. A mechanism used to identify and isolate the sources of hard errors on a token-ring network

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few

instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

C

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

concentrator. A single-protocol networking device, such as the 8239.

Configuration Report Server. A function of the token-ring manager that accepts commands to get station information, set station parameters, and remove stations on its ring. It also collects and forwards configuration reports generated by station on its ring to the LAN manager.

CRS. Configuration Report Server.

D

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

E

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

H

hub. A multiprotocol-networking device that can contain modules supporting concentrators, bridges, routers, and so on, such as the 8239. A hub is also referred to as a *stack unit*.

HyperText Markup Language (HTML). A markup language that is specified by an SGML document type definition (DTD) and that is understood by all World Wide Web servers.

I

in-band. The ability to manage an 8239 remotely by communicating over the token-ring data network.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

L

LCD. Liquid crystal display.

LED. Light emitting diode

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Synonymous with *remote*.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*.

M

MAC. Imedium access control.

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

markup language. An application-oriented language designed to transform raw text into structured documents by inserting procedural and descriptive markup into the raw text. Examples of markup languages are HTML, DCF, PAGE, SCRIBE, SCRIPT, and SGML.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

Medium Access Control (MAC). The sublayer of DLC that supports medium-dependent functions and uses the services of the physical layer to provide services to Logical Link Control (LLC).

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

N

network interface card (NIC)). The point of interconnection between the public switched network and a privately owned terminal.

O

out-of-band. The ability to manage the 8239 by attaching the device to the EIA-232 interface on the stack unit. The data does not go across the data network.

P

packet internet groper (PING). A program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply.

phantom voltage. A DC voltage superimposed on a Token-Ring signal; it is used to signal a Token-Ring concentrator that a station is ready to be inserted into the ring.

R

REM. Ring Error Monitor.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

ring error monitor (REM). A function of the token-ring manager that observes, collects, and analyzes recoverable and irrecoverable error reports sent by token-ring stations on a single token-ring network and assists in fault isolation and correction.

Ring Parameter Server (RPS). This function resides on each ring for which operational parameters are being managed. It sends initialization information to new stations attaching to the ring, makes sure that stations on the ring have consistent values for operational parameters, and forwards registration information to LAN managers from stations attaching to the ring.

RPS. Ring Parameter Server.

S

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

soft error. An intermittent error on a network that causes data to have to be transmitted more than once to be received. A soft error does not, by itself, affect the network's overall reliability. If the number of soft errors reaches the ring error limit, reliability is affected.

stack. A single 8239 system containing one or more stack units that are connected using Stack In/Stack Out connectors.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

subnetwork mask. Synonym for *address mask*.

T

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trivial File Transfer Protocol (TFTP). A protocol that transfers files between hosts using minimal protocol.

U

uniform resource locator (URL). For HTML documents and for the World Wide Web, a sequence of characters that represent information resources. This sequence of characters includes (a) the abbreviated name of the protocol used to access the information resource and (b) the information used by the protocol to locate the information resource.

User Datagram Protocol (UDP). (1) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. UDP is used for application-to-application programs between TCP/IP host systems. (2) The Internet Protocol that enables an application programmer on one machine or process to send a datagram to an application program on another machine or process. UDP uses the internet protocol (IP) to deliver datagrams.

W

web browser. A client program that allows a user to navigate the Internet World Wide Web via hypertext links. These links, called uniform resource locators (URLs), specify the protocol, location, and file name of each document. The documents can be text, graphics, video, or audio.

World Wide Web (WWW). (1) A global, interactive, dynamic, cross-platform, distributed graphical hypertext information system that runs over the Internet. (2) An internation, virtual-network-based information service composed of internet host computers that provide online information in a specific hypertext format. (A)

X

XMODEM. A public-domain asynchronous data link control (DLC) protocol that provides packet numbering and checksum error control for the transfer of binary files.

Index

Numerics

A

B

C

D

E

F

I

L

Communicating Your Comments to IBM

8239 Token-Ring Stackable Hub
Setup and User's Guide

Publication No. GA27-4209-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  1-800-253-3520

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Readers' Comments — We'd Like to Hear from You

8239 Token-Ring Stackable Hub
Setup and User's Guide

Publication No. GA27-4209-01

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
GA27-4209-01

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in USA

GA27-4209-01

Spine information:

IBM 8239 Token-Ring Stackable Hub Setup and User's Guide