Ethernet Stackable Hub 8245
Models 012, 024, 112, and 124

Installation and Planning Guide

Note:

Before using this information and the product it supports, be sure to read the safety information under "Safety Information" on page xiii and the general and emission notices in Appendix A.

Second Edition (April 1999)

This edition applies to Version 1.10 of IBM 10/100 Ethernet Stackable Hub 8245.

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

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

Department CGF
Design & Information Development
IBM Corporation
PO Box 12195
Research Triangle Park NC 27709-9990
USA

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

Chapter 3. Control Panel Management

Chapter 4. Using the Management Interface

Chapter 5. Using Web Management

Chapter 6. Troubleshooting and Service

Appendix A. Notices

Appendix B. Cable Pinout Diagrams

Figures

Tables

Safety Information

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.

Gevarr: Voodrat 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'nstallation 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 instaler deste produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança–Leia 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 pöcnete sa instalacijom produkta, procitajte naputak o pravilima o sigurnom rukovanju u Upozorenje: Pravila o sigurnom rukovanju - Prvo procitaj ovo, SD21-0030. Ovaj privitak opisuje sigurnosne postupke za priključrivanje kabela i priključivanje na elektricno napajanje.

Upozornění: než zahájíte instalaci tohoto produktu, přečtěte si nejprve bezpečnostní informace v pokynech, Bezpečnostní informace, SD21-0030. 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.

Gevarr: 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.

VARRA: Ennen kuin aloitat tämän tuotteen asennuksen, lue julkaisussa *Varoitus: Turvaohjeet–Lue tämä ensin,* SD21-0030, olevat turvaohjeet. Tässä kirjasessa on ohjeet siitä, mitensähkölaitteet 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 équipments électriques en toute sécurité.

Vorsicht: Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen–Bitte zuerst lesen*, SD21-0030. Diese Veröffentilchung beschreibt die Sicherheitsvorkehrungen für das Verkabien 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, miyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.

Pericolo: prima di iniziare l'installazione di questo prodotto, leggere le informazioni relatie alla sicurezza riportate nell'opuscolo *Attenzione: Informazioni di sicurezza–Prime informazioni da leggere,* SD21-0030, 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 forst*, 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: Säkerhetsforeskrifter – Läs detta först*, SD21-0030. Där beskrivs hur du på ett säkert satt 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。

About This Manual

This manual explains how to install and service the IBM Ethernet Stackable Hub 8245 Models 012, 024, 112 and 124.

Who Should Read This Manual

This manual is intended for use by installation technicians, network administrators, and service personnel.

How This Manual Is Organized

- Chapter 1, “Introduction” provides a functional product description and cabling requirements.
- Chapter 2, “Installation” describes installation and cabling procedures.
- Chapter 3, “Control Panel Management” describes how to use the Ethernet Stackable Hub control panel.
- Chapter 4, “Using the Management Interface” describes how to use the EIA 232 management port through a local connection.
- Chapter 5, “Web Management” describes how to use an Internet Web browser to connect to and manage your Ethernet Stackable Hub.
- Chapter 6, “Troubleshooting” provides troubleshooting procedures, how to get help from IBM, and procedures for downloading new code.
- Appendix A, “Notices” describes product notices and provides warranty information.
- Appendic B, “Cable Pinout Diagrams” shows cable and pin configurations.

Prerequisite Publication

Caution: Safety Information - Read This First, SD21-0030.

Chapter 1. Introduction

This chapter describes the features of the IBM 10/100 Ethernet Stackable Hub 8245, Models 012, 024, 112, and 124. It provides a functional overview that can help you integrate the 10/100 Ethernet Stackable Hub into your new or existing network.

The 10/100 Ethernet Stackable Hub 8245 is a 10BASE-T/100BASE-TX dual-speed intelligent Ethernet hub. The 10/100 Ethernet Stackable Hub 8245 consists of 12-port and 24-port managed and manageable units with many features that make monitoring, configuring and expanding a LAN easy and efficient.

The 10/100 Ethernet Stackable Hub 8245 is designed for use in medium-sized workgroups or remote locations that are part of a large campus network.

The 10/100 Ethernet Stackable Hub 8245 series has four models, two managed hubs with 12 and 24 ports (Models 112 and 124) and two manageable hubs with 12 and 24 ports (Models 012 and 024). One managed hub can manage all the hubs in a stack. Manageable hubs can be stacked without a managed hub and work without management features.

Managed Models

Managed Models 112 and 124 display system and port information in the control panel as shown in Figure 1-1 and Figure 1-2.

Figure 1-1 10/100 Ethernet Stackable Hub 8245 Model 112

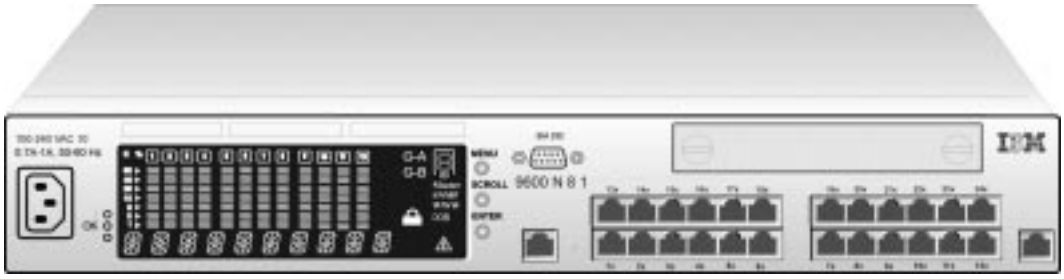


Figure 1-2 10/100 Ethernet Stackable Hub 8245 Model 124

Manageable Models

Manageable Models 012 and 024 indicate their port status through an LED panel with LEDs for every port indicating link status (Link/Rx) and port speed (10 Mbps/100 Mbps) as shown in Figure 1-3 and Figure 1-4. Utilization is indicated by five graduated LEDs and collisions are indicated by a Collision LED for each segment.

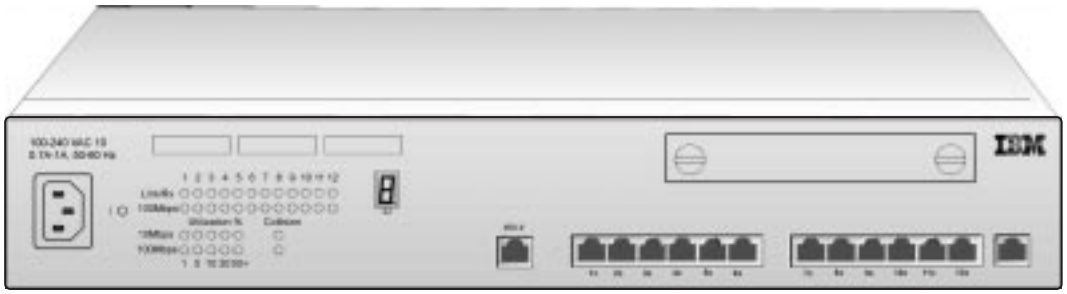


Figure 1-3 10/100 Ethernet Stackable Hub 8245 Model 012

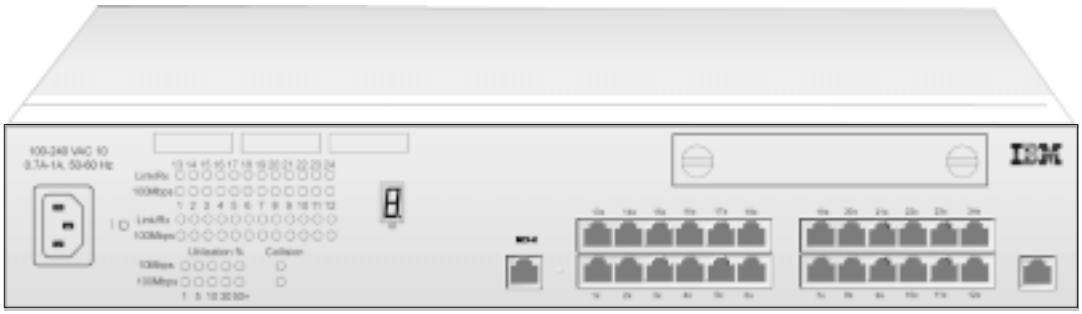


Figure 1-4 10/100 Ethernet Stackable Hub 8245 Model 024

Product Features

Models 012 and 024

- 12/24 MDI-X 10BASE-T/100BASE-TX ports with shielded RJ-45 connectors
- Two MDI ports that share ports 1 and 12 and use shielded RJ-45 connectors
- All ports use UTP/STP cable - Category 3, 4, or 5 for 10 Mbps, Category 5 for 100 Mbps
- All ports support auto-partition/reconnect capability
- All ports support auto-polarity reversal
- Jabber protection
- Hub ID indicator is automatically set by stack position
- Compliance with IEEE802.3 10BASE-T standard
- Compliance with IEEE802.3u 100BASE-TX standard
- Compliance with IEEE802.3u 100BASE-FX standard (optional module)
- Compliance with IEEE802.3 repeater standard
- Per-port status LED (Link, Rx, and Speed)
- Per-segment collision LED
- Per-segment utilization indicator
- An optional module slot for one of the following modules:
  - A 10/100 bridge with 10BASE-T/100BASE-TX Uplink
  - A 10/100 bridge with 100BASE-FX Uplink
  - An AUI Expansion Module
- Support for hot-swap with the Stack Link Cable (with Software Version 1.10 and later)

Models 112 and 124

These models include the features of Models 012 and 024 (except LEDs) plus the following features:

- Support for the Backup Managed function, which allows more than one managed unit in a stack. This feature will back up configuration data from an active managed unit to the backup managed unit to provide the protection against power failure on Managed unit or damage to the Stack Link Cable (with Software Version 1.10 and later)
- Support for Hot-Swap with the Stack Link Cable (with Software Version 1.10 and later)

- One EIA 232 Management Port (DTE male), which supports local console management or out-of-band management
- Network utilization indicators for both 10-Mbps and 100-Mbps segments
- Management function through the control panel
- Support for in-band Telnet, SNMP, and Web-based management capability
- Support for software upgrade capability through the standard TFTP protocol
- Support for RFC1213 MIB-II, RFC1516 Repeater MIB, RFC1757 RMON MIB (Group 1, 2, 3, and 9), and proprietary MIB
- Support for traps to report the hub event to the specified SNMP managers and Web-based manager
- Group/port control and status monitoring capability
- Statistics counter monitoring capability
- RMON (Group 1, 2, 3, 9) probe capability
- Redundant link capability
- Security (intrusion) control capability
- Address (source MAC address) tracking capability
- Address (source MAC address) searching capability
- Broadcast storm protection
- BootP Protocol

Functional Characteristics

Figures 1-5 and 1-6 identify the components of the 10/100 Ethernet Stackable Hub.

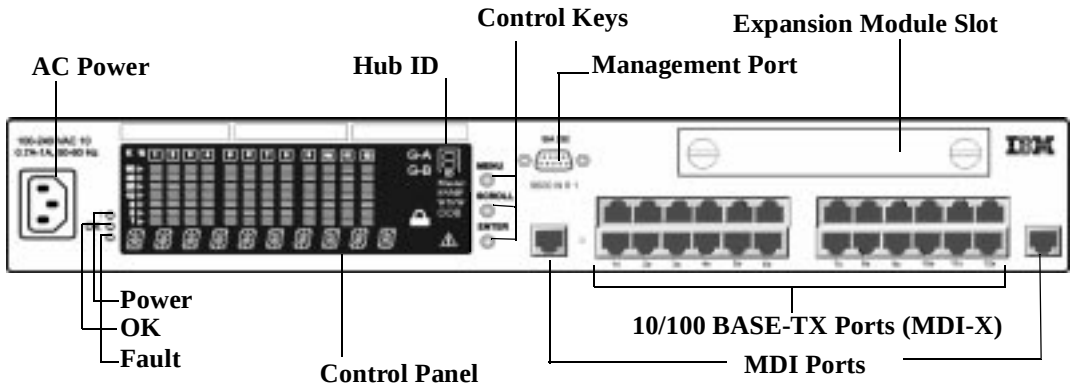


Figure 1-5 Model 124 Front Panel

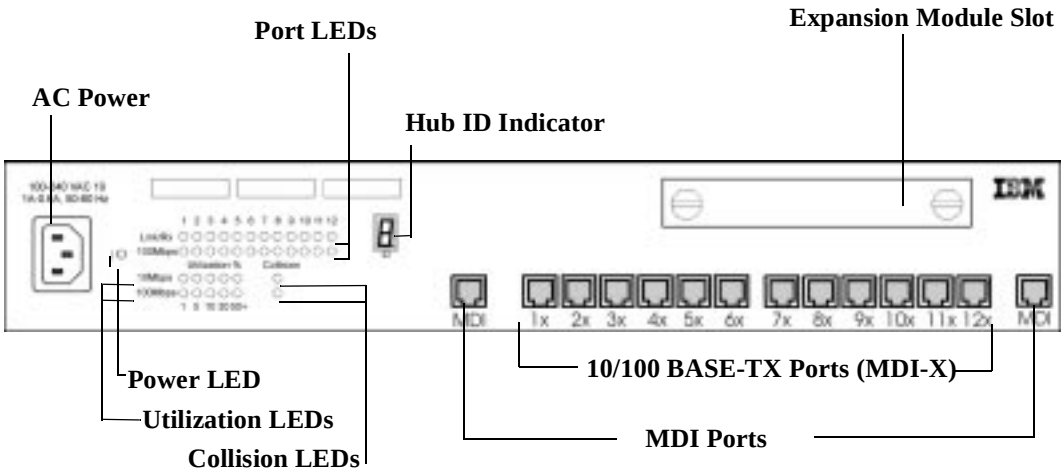


Figure 1-6 Model 012 Front Panel

Status and Activity Indicators

Manageable Models 012 and 024 indicate their port status with different colors or flashing LEDs for each port. LED traffic statistic information is indicated by five graduated Utilization LEDs, one for 10 Mbps and another for 100 Mbps communications. Each 10-Mbps and 100-Mbps segment has its own Collision LED.

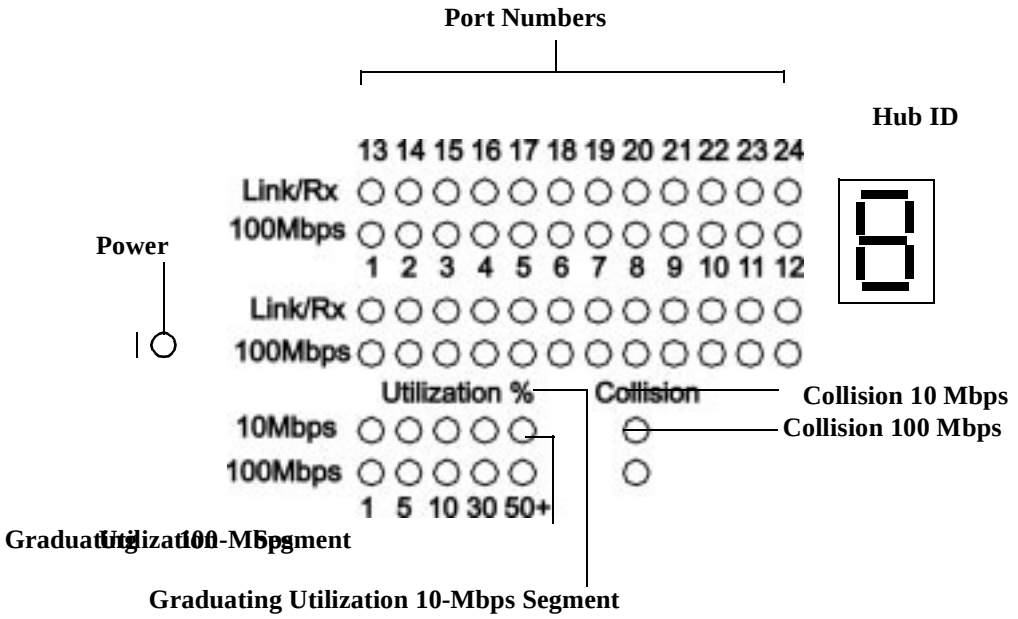


Figure 1-7 LEDs for the Manageable Models

Table 1-1 LED Indicators and Meanings

LED	Status	Meaning
Power	On	There is power to the hub.
Utilization	On	Indicates percentage of utilization with an array of LEDs. The number below the LED indicates the percentage of hub capacity being used. For example, if all five LEDs are on, the hub is being heavily utilized. Data traffic within the hub is 50% (or more) of its capacity.
Collision	On	There are collisions on the 10-Mbps or 100-Mbps segment.
Link/Rx	On	The port is linked.
Link/Rx	Blinking	The port is receiving data.
Link/Rx	Off	This port is in link down state, auto-partitioned, or disabled by the administrator.
100-Mbps	On	The port speed is 100 Mbps.
100-Mbps	Off	The port speed is 10 Mbps.

Control Panel

The control panel, shown in Figure 1-8, provides overall utilization statistics that allow you to monitor all the ports at a glance, as well as detailed error and configuration information by port.

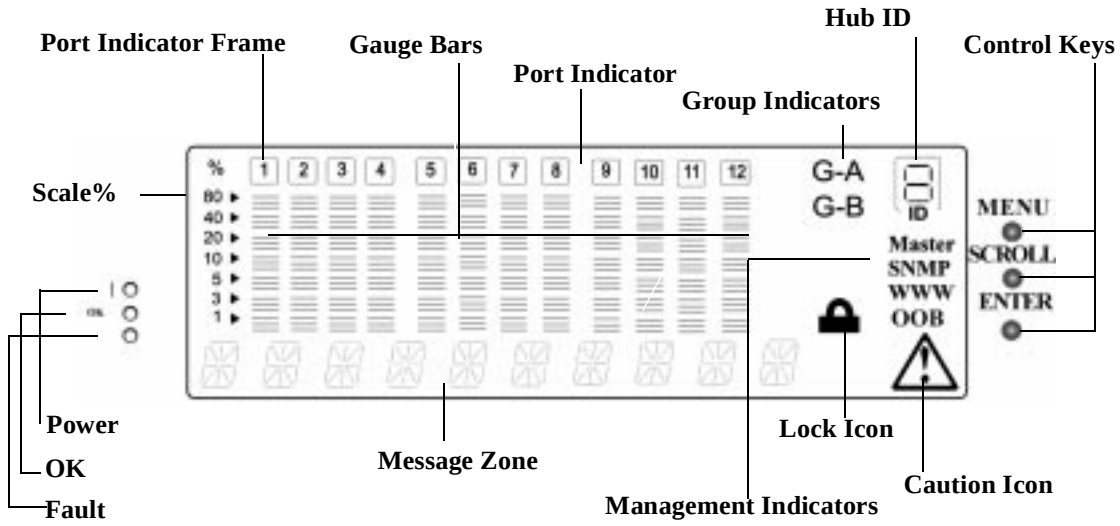


Figure 1-8 Control Panel

Power

Indicates that power is connected.

OK

Indicates that the POST was run without errors.

Fault

Indicates that the POST found an error.

Scale %

Indicates the relative percentage of utilization or collision. Each port has its own percentage scale.

Port Indicator

Indicates a port number.

Port Indicator Frame

Indicates which ports are disabled.

Message Zone

Displays test messages, the menu items, and status information:

- **Active managed unit:** displays ***Utilization*** and ***10M 100M***.
- **Backup managed unit:** displays its current mode, ***Backup Mode***.
- **Manageable unit:** displays its current mode, ***Manageable Mode***.

Gauge Bars

Display port-related information such as utilization.

Lock Icon

Indicates that the control panel configuration is locked.

G-A

Displays status of ports 1 to 12 in Port Group A.

G-B

Displays status of ports 13 to 24 in Port Group B.

Master

Indicates that the hub is a managed hub.

SNMP

Indicates that the hub is SNMP-manageable.

WWW

Indicates that the Web Management feature is enabled.

OOB

Indicates that out-of-band is enabled.

CAUTION ICON

Indicates that an error has occurred.

Hub ID

The 10/100 Ethernet Stackable Hub ID is automatically set based on the stack position. Each hub that is added to the stack is assigned a Hub ID from 1 to 6 depending on its position in the stack.

Note: If the Hub ID changes (for example, the hub's position in the stack changes), the hub performs a warm start automatically.

Control Keys

The control keys are used to cycle through the menus and make selections.

The following table summarizes the control keys functions:

Table 1-2 Control Keys

MENU	Return to the previous level
SCROLL	Choose another topic within the same level
ENTER	Go to the next level, view status, or confirm the configurable settings

Note: For a backup managed unit, use the control keys only to switch the display of port status from Port Group A to Port Group B.

Communication Ports

- Ethernet Ports: 12/24 MDI-X 10BASE-T/100BASE-TX Ethernet. All ports use UTP/STP Category 3, 4, or 5 cables with RJ-45 connectors for 10 Mbps and Category 5 cable for 100 Mbps.
- MDI Ports: Two shared ports: one shared with port 1 and one shared with port 12. The MDI ports take priority when shared with ports 1 and 12. These ports use UTP/STP Category 3, 4, or 5 cables with RJ-45 connectors for 10 Mbps and Category 5 cable for 100 Mbps.
- Expansion Ports: One expansion slot is located on the front panel. This slot allows you to add a 100BASE-FX uplink, a 10BASE-T/100BASE-TX uplink, or an AUI Expansion Module.

Management Port

The management port is an EIA 232 (formerly RS232-C) serial interface that you use to configure the 10/100 Ethernet Stackable Hub 8245. You can connect a terminal emulator to this port for local console or out-of-band (SLIP) management.

VT-100 terminal connection to the management port requires the following settings:

Baud rate: 9600 bps
Character size: 8 data bits per character
Stop bits: 1 stop bit
Parity bit: no parity

For out-of-band (SLIP) management you can configure the management port using the local console/remote Telnet, the Web-based manager, or the SNMP manager using the following settings:

Baud rate: 2400, 4800, 9600, or 19200 bps
Character size: 8 data bits per character
Stop bits: 1 stop bit
Parity bit: no parity

Optional Modules

Three types of optional expansion modules are available for the 10/100 Ethernet Stackable Hub 8245. You can insert these modules into the expansion slot that is located on the front panel of the hub. The modules are:

- **10/100 Bridge with 10BASE-T/100BASE-TX Uplink Module** as shown in Figure 1-9. This module supports store and forward and back-pressure for both internal and external bridges.

  The TX module's internal bridge enables the hub to pass data between 10-Mbps and 100-Mbps segments. The external bridge allows you to cascade other stacks through its 10/100-TX uplink.

- **10/100 Bridge with 100BASE-FX Uplink Module** as shown in Figure 1-10. This module supports store and forward and back-pressure for both internal and external bridges.

  The FX module's internal bridge enables the hub to pass data between 10-Mbps and 100-Mbps segments. The external bridge allows you to cascade other stacks through its FX uplink using fiber cable. FX connections allow cable lengths up to 2 km (1.2 miles) when operating in full-duplex mode and 412 m (1352 ft) when operating in half-duplex mode.

- **AUI Expansion Module** as shown in Figure 1-11. This module attaches to the 10-Mbps segment and supports half-duplex mode for connection to a 10BASE5, 10BASE2, or 10BASE-F network segment using the appropriate transceiver.

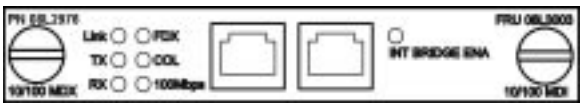


Figure 1-9 10/100 Bridge with 10BASE-T/100BASE-TX Uplink

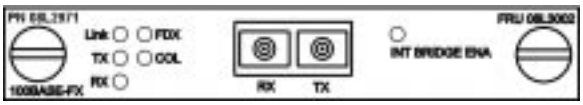


Figure 1-10 10/100 Bridge with 100BASE-FX Uplink

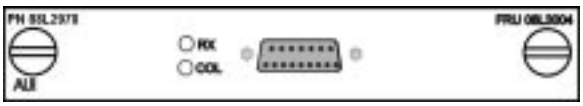


Figure 1-11 AUI Expansion Module

Physical Characteristics and Requirements

Power Requirements

- A standard ac power cord
- Input voltage: 100 V ac to 240 V ac
- Input frequency: 50 Hz to 60 Hz
- Input current max: 1 A at 100 V ac or 0.7 A at 240 V ac

Operating Environment

Table 1-3 Operating Environment

Environment	Ambient Temperature	Relative Humidity	Wet Bulb Temp.
Power on	10° to 40° C (50° to 104° F)	8 to 80%	27° C
Storage	-25° to 70° C (-13° to 158° F)	5 to 80%	29° C
Shipment	-40° to 60° C (-40° to 140° F)	5 to 100%	29° C

Physical Dimensions

Table 1-4 Physical Dimensions

Width	439.4 mm (17.3 in.) 1.5U rack mountable
Height	64 mm (2.5 in.)
Length	217 mm (8.5 in.)
Weight for Models 012, 024	3.6 kg (7.9 lb)
Weight for Models 112, 124	3.8 kg (8.4 lb)

Power Dissipation

47 watts maximum (160 BTU per hour)

dB Rating

40 dB

EMC Certifications

- FCC Class A
- CISPR-22 Class A

Safety Certifications

- UL 1950
- CSA
- IEC 950
- CB Bulletin

Chapter 2. Installation

This chapter describes installation procedures. Before installing the 10/100 Ethernet Stackable Hub 8245, be sure to read the "Safety Information" on page xiii and the notices and warranty information in Appendix A "Notices."

Installation Summary

Table 2-1 Ethernet Stackable Hub Installation Procedures

Step	Procedure	Reference
1.	Read the safety information booklet shipped with the Ethernet Stackable Hub	SD21-0030
2.	Unpack the 10/100 Ethernet Stackable Hub	See page 2-1
3.	Arrange the position of managed and manageable units	See page 2-3
4.	Tabletop-mount the 10/100 Ethernet Stackable Hub	See page 2-5
5.	Rack-mount the 10/100 Ethernet Stackable Hub	See page 2-6
6.	Install an optional module	See page 2-7
7.	Attach the stack link cable	See page 2-10
8.	Perform power-on checkout	See page 2-11
9.	Connect the cables	See page 2-12
10.	Configure the 10/100 Ethernet Stackable Hub	See page 2-13

Unpacking Instructions

Step 1. Verify that the following items are in the package along with this manual:

- An IBM Ethernet Stackable Hub 8245
- Two rack-mounting brackets and 8 screws
- A power cord
- A stack link cable
- *8245 Quick Reference Guide* (preinstalled in card tray beneath the Ethernet Stackable Hub)
- *Caution: Safety Information - Read This First*

- *8245 Quick Installation Guide*

Step 2. Visually inspect the unit to ensure that it was not damaged during shipping. If any items are missing or damaged, contact your place of purchase.

Instructions for Installing Managed Units

With Software Version 1.10 and later, the managed units support the backup managed function to provide the protection against power failure on Managed unit or damage to the Stack Link Cable. With this function, you can place more than one managed unit in a stack of hubs. Only the managed unit at the top of the stack (active managed unit) can manage other units. The managed unit below it will be the backup managed unit. Any other managed units in the stack will function as manageable units. The managed unit copies parts of the configuration to the backup managed unit every 30 minutes or during a restart. For data that is not copied, see Table 2-2 on page 2-4. If the backup managed unit senses that the managed unit has lost management capability, it will perform a warm start and boot up as the new active managed unit. When the backup managed unit becomes the active managed unit in the stack it will have the managed unit's original configuration data. Data is copied only from the managed unit to the backup managed unit.

Note: It is better to upload and save the configuration of the current managed unit to a TFTP server periodically or before installing a new managed unit. You will be able to restore the original configuration if any critical operation causes the loss of the old settings.

To install multiple managed units, do the following steps:

Step 1. Check all the software versions of the managed units to verify all units have the same level of code, and that the level of code is Version 1.10 or later.

Step 2. Configure the managed units for Backup Managed Function. See "Adding and Replacing Units in the Stack" on page 2-17.

Step 3. Put all the managed units above the manageable units.

Step 4. Connect all the stack link cables to each hub.

Step 5. Connect the power for each hub from top to bottom.

Requirements for the backup managed function:

1. With this function, the managed units should always be above the manageable units. Otherwise, the managed unit operates as a manageable unit if it is stacked under a manageable unit.
2. In order to have the same database structure to duplicate the configuration from the active managed unit to the backup managed unit, the active managed unit and backup managed unit need to have the same level of the software.
3. The active managed unit and the backup managed unit must each have a unique IP address.

Table 2-2 Data that Cannot be Copied from the Managed Unit to the Backup Managed Unit

Category	Items
User Information	User Name User Password
Network Management Ethernet	IP Address Subnet Mask Default Gateway Bootp Selection
Network Management OOB	IP address Subnet Mask Speed
TFTP	File name of Runtime File name of Bootload File name of Web Page File name of Configuration IP address of TFTP server (see note)
System Information	Location Name Contact SNMP community Timeout Interval of Telnet login

Note: When a system download was run on the active managed unit and the software version is different from the one on the backup managed unit, the IP address of the TFTP server will then be copied to the backup managed unit.

Tabletop Mounting the 10/100 Ethernet Stackable Hub

The 10/100 Ethernet Stackable Hub 8245 can be installed on a flat level surface. To install the 10/100 Ethernet Stackable Hub on a flat level surface, refer to Figure 2-1 which provides the clearance information for all sides of the 10/100 Ethernet Stackable Hub.

Front — Adequate room to view control panel display

Side — 50.8 mm (2 in.)

Rear — 127 mm (5 in.)

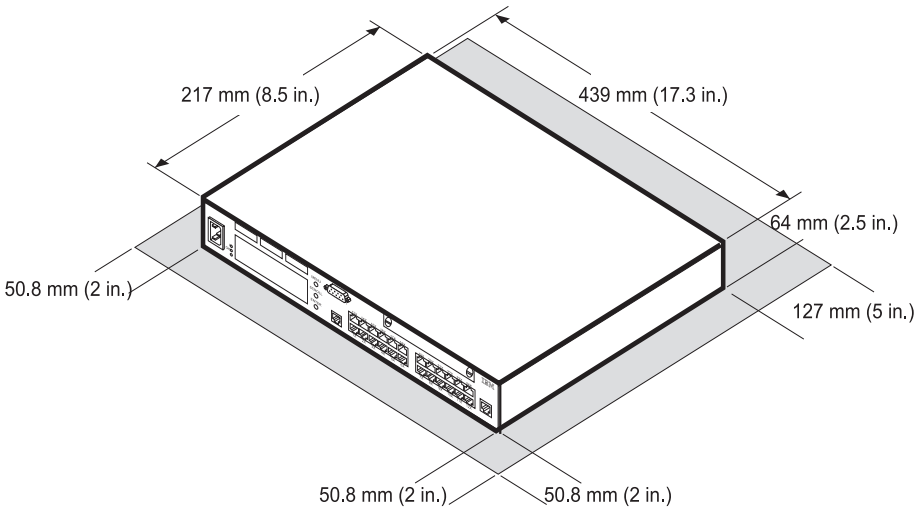


Figure 2-1 Tabletop Mounting the 10/100 Ethernet Stackable Hub

Rack-Mounting the 10/100 Ethernet Stackable Hub 8245

Follow these steps to mount the 10/100 Ethernet Stackable Hub in a rack:

Step 1. Install the two mounting brackets on the sides of the Ethernet Stackable Hub using the brackets and screws provided.

Step 2. Insert the hub into a 19-inch rack.

Note: Ensure that the ventilation holes are not obstructed. The screws for rack-mounting are not provided.

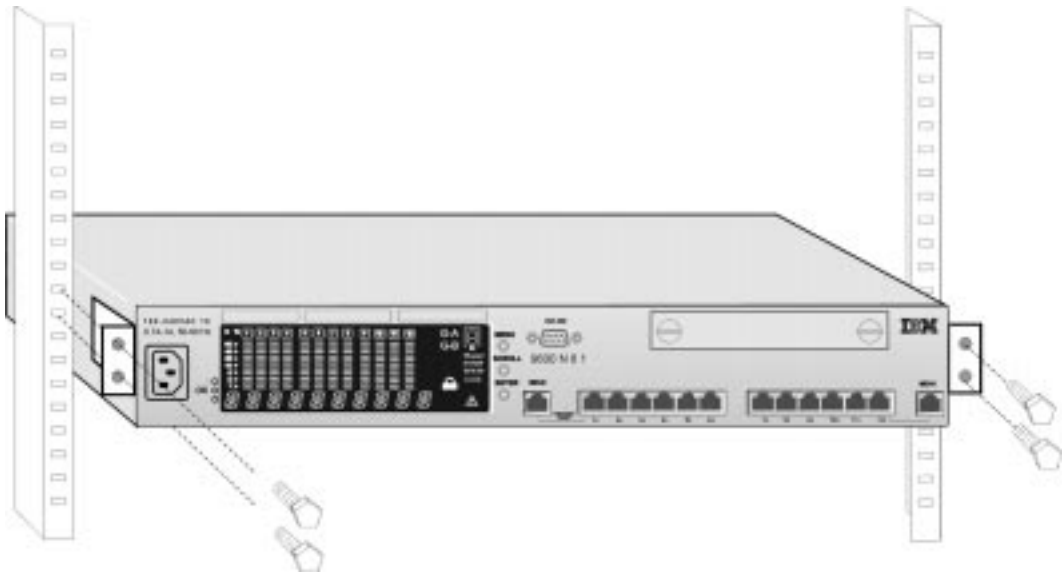


Figure 2-2 Rack-Mounting the 10/100 Ethernet Stackable Hub

Installing an Optional Module

Power off the Ethernet Stackable Hub before installing an optional expansion module.

Three optional bridge modules are available for the 10/100 Ethernet Stackable Hub 8245:

- 10/100 Bridge with 10BASE-T/100BASE-TX Uplink Module (PN 08L2976).
- 10/100 Bridge with 100BASE-FX Uplink Module (PN 08L2971). This module uses SC-type connectors with multi-mode fiber.
- AUI Expansion Module (PN 08L2978). See Note 4.

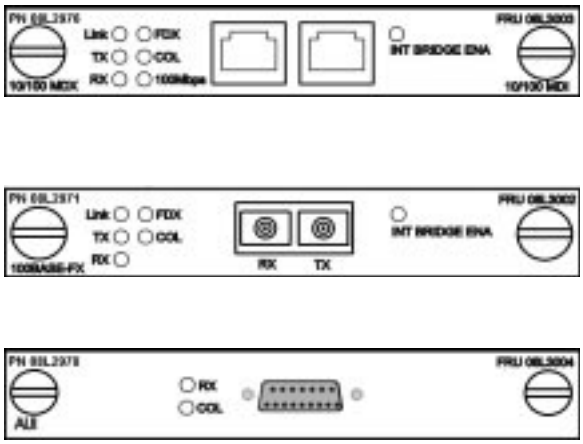


Figure 2-3 10/100-TX Bridge Module, 100BASE-FX Bridge Module, and AUI Expansion Module

Notes:

1. Modules are not hot-swappable. Remove power from the hub before installing or replacing a bridge module.
2. You should enable the internal bridge on only one bridge module when you have multiple bridge modules installed in a stack. This prevents a network loop condition.
3. The TX and FX Uplink modules are shipped with the internal bridge disabled.
4. Before installing the AUI Module, ensure that you have Version 1.06 or later System Software (Run-Time), Version 1.03 or later BOOT ROM, and Version 1.03 or later Web-Pages installed on all managed units (model 112 and 124) in the stack.

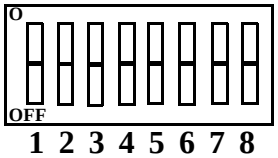
To install these modules, perform the following steps:

Step 1. Set the DIP Switch for the internal bridge. See Figures 2-4 and 2-5 for the correct switch settings.

DIP Switch Setting for the 10/100 Bridge with 10/100-TX Uplink Module

DIP 1 to 4 Set to ON to enable the internal bridge.

DIP 5 to 8 Not used.



	DIP1	DIP2	DIP3	DIP4
Internal Bridge Enable	**ON**	**ON**	**ON**	**ON**
Internal Bridge Disable	**OFF**	**OFF**	**OFF**	**OFF**

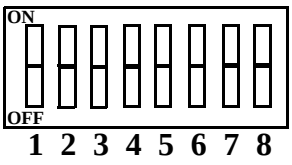
Figure 2-4 TX Module DIP Switch Setting

DIP Switch Setting for the 10/100 Bridge with 100BASE-FX Uplink Module

DIP 1 to 4 Set to ON to enable the internal bridge.

DIP 5 Set to ON/OFF to enable FX half duplex/full duplex.

DIP 6 to 8 Not used.



	DIP1	DIP2	DIP3	DIP4	DIP5
Internal Bridge Enable	**ON**	**ON**	**ON**	**ON**	
Internal Bridge Disable	**OFF**	**OFF**	**OFF**	**OFF**	
FX Half Duplex					**ON**
FX Full Duplex					**OFF**

Figure 2-5 FX Module DIP Switch Setting

Step 2. Remove the power from the 8245 by disconnecting the power cable from the ac outlet.

Step 3. Remove the installed bridge module or blank cover by turning the two knobs on the front counterclockwise as shown in Figure 2-6.

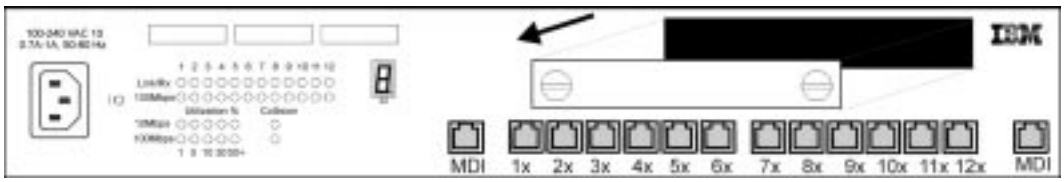


Figure 2-6 Removing the Blank Module Panel

Step 4. Insert the new module, ensuring that the edges slide through the guides, as shown in Figure 2-7.

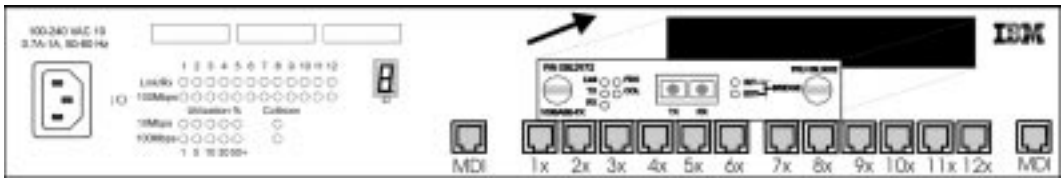


Figure 2-7 Inserting the Module

Step 5. Turn the two knobs on the new bridge module clockwise until they are securely attached to the 8245.

Step 6. Connect the appropriate communication cable to the new module.

Step 7. Reconnect the ac power cord to the wall outlet.

For information about attaching cables to the newly installed expansion module, see “Cabling” on page 2-12.

Stacking Hubs with Stack Link Cables

Hubs can be stacked by using stack link cables (FRU 25L4900). These cables extend the number of ports on a segment beyond the limit afforded by a single hub. You can stack up to six Ethernet Stackable Hubs using stack link cables.

The 8245 112/124 hubs support hot-plugging with the stack link cables and multiple managed units in a stack with Software Version 1.10 and later. You can plug in the stack link cables without disconnecting the power from each unit.

Each hub is identified by a unique Group Software ID, even though a new hub is added into the stack and the hub ID of all the hubs in the stack can change, the original configurations and settings of the hubs are unaffected and, therefore, remain the same.

Notes:

1. Managed units must be at the top of the stack.
2. Be careful when connecting and disconnecting the stack link cables to prevent accidental bending or breaking of the signal pins. (See Figure 2-8, “Stacking Hubs with Stack Link Cable,” on page 2-10.)
3. The response time for the managed unit to update the database is approximately 10 seconds.

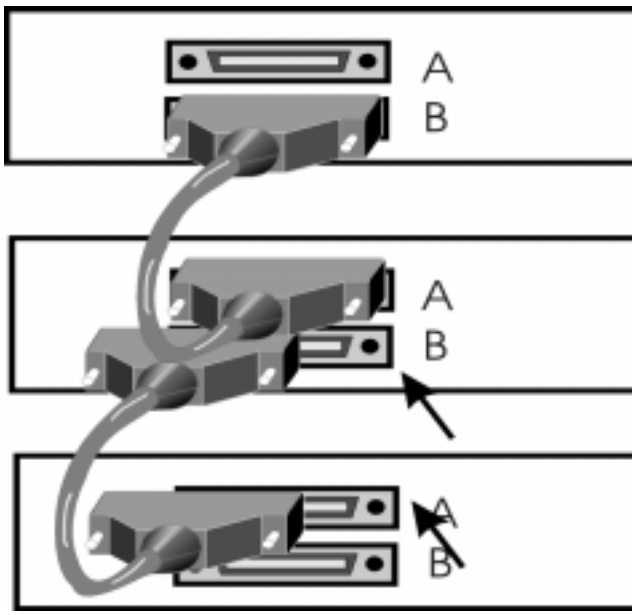


Figure 2-8 Stacking Hubs with Stack Link Cable

Power-On Checkout

Connect the ac power cable from the front panel to the power source. This powers on the Ethernet Stackable Hub.

When the managed Ethernet Stackable Hub is powered on it runs a power-on self-test (POST). Tests such as NMU mode, test EEPROM, and test NIC are run. A display area on the control panel called the *message zone* indicates the particular test being run. If all the tests pass, a final result SELF TEST OK is displayed in the message zone. After the POST completes, the control panel defaults to UTILIZATION status. If a test detects an error during the POST, an error message is displayed. See Chapter 6 “Troubleshooting and Service,” for more information on error messages.

Cabling

Cable Tips:

- Avoid stretching or bending cables.
- Avoid routing cables near potential sources of electromagnetic interference, such as motorized devices or fluorescent lights.
- Route cables away from aisles and walkways to avoid creating trip hazards. Use floor cable covers to secure cables if such routes cannot be avoided.

Attaching Cables to Ports

Step 1. Refer to your network documentation to determine each cable's port or expansion slot assignment.

Step 2. Using appropriate connectors, connect the cables to the ports or expansion slots.

Step 3. Start by labeling each end of the cable. This will simplify network troubleshooting later. As a minimum, we suggest a label containing:

At the hub end of the cable:

- A unique identifier for the cable
- Location of the far end of the cable
- MAC address of the device at the far end of the cable

At the opposite end of the cable:

- The port number to which the cable is attached

Connecting a PC to the Management Port

To access the managed hub's local terminal, perform the following steps:

Step 1. Connect one end of a null-modem cable (direct connection) to the Ethernet Stackable Hub management port labeled EIA 232 (see Figure 2-9).

Step 2. Connect the other end to the communication port on your PC.

For information on setting up a session through the management port, see "Setting Up a Management Session" on page 4-1.

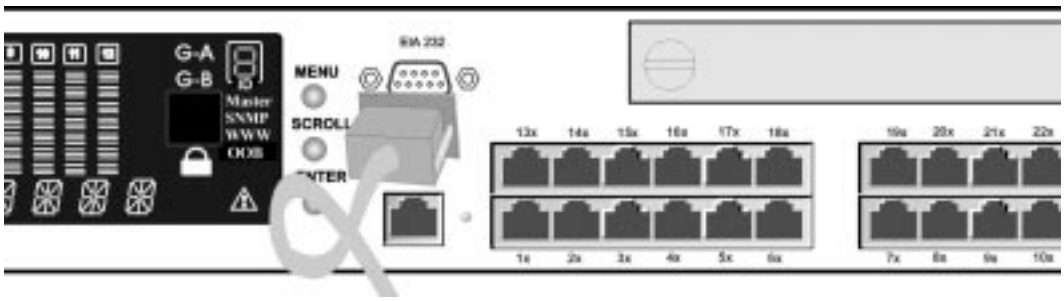


Figure 2-9 Connecting to the Management Port

Ethernet Connections

To connect a workstation to the Ethernet Stackable Hub, connect one end of the UTP/STP cable to a workstation's Ethernet RJ-45 port and the other end to a port on the hub.

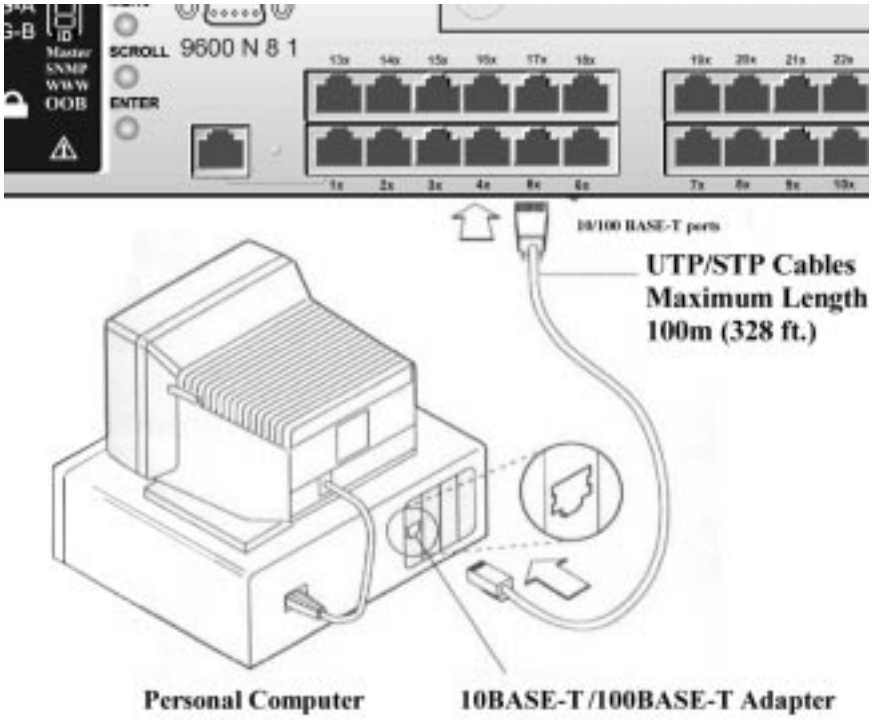


Figure 2-10 Connecting Workstations

The maximum length of cable between the Ethernet Stackable Hub and other devices is 100 m (328 ft).

Connecting a Modem

Connect one end of a serial cable (direct connection) to a modem and the other end to the management port of the 10/100 Ethernet Stackable Hub.

Cables and Distances between Devices

Devices attached to the front of the Ethernet Stackable Hub using UTP/STP Category 3, 4, or 5 cabling follow the rules established in the IEEE 802.3 standard for 10BASE-T Ethernet implementation.

Straight-Through Cables

All the front panel ports, including the MDI ports, use straight-through cables to attach devices.

Crossover Cables

Crossover cables are used when linking MDI to MDI ports or MDI-X to MDI-X ports.

Maximum Cable Lengths

Table 2-3 lists the maximum recommended cable lengths between the 10/100 Ethernet Stackable Hub and workstations.

Table 2-3 Recommended Maximum Cable Lengths

Ethernet Type	Maximum Segment Length
10BASE-T	100 m (328 ft)
100BASE-TX (hub to workstation)	100 m (328 ft)
100BASE-TX (hub to hub via repeater port)	5 m (16.4 ft)
100BASE-TX (hub to hub via bridge modules)	100 m (328 ft)
100BASE-FX	Half duplex - 412 m (1352 ft) Full duplex - 2000 m (6560 ft)

Cabling Requirements

10BASE-T ports will operate correctly on any of the following cables:

- Category 3, 4, or 5 100-ohm UTP or STP cable and connection hardware as specified in the ANSI/TIA/EIA 568-A or CSA T529 standards.
- 150-ohm STP-A cable and components as specified in the ANSI/TIA/EIA 568-A or CSA T529 standards.
- IBM Cabling System types 1, 6, and 9, 150-ohm STP-A cable. If you are using 150-ohm cabling systems, impedance-matching devices must be used in conjunction with the cable.
- Category 3, 4, or 5 100-ohm and 120-ohm, balanced, shielded or unshielded cables and components as specified in the ISO/IEC 11801 standards.

- 150-ohm, balanced, shielded or unshielded cables and components as specified in the ISO/IEC 11801 standards.
- Any link that meets the specifications of a Class D link. If you are using 150-ohm cabling systems, impedance-matching devices must be used in conjunction with the cable.

Notes:

1. All devices connected to the cables must be grounded.
2. Do not use telephone extension cables in 10BASE-T networks. The wire pairs in those cables are not twisted and the cable does not meet other requirements for use in a 10BASE-T network.

100BASE-TX ports require the following cable:

- Class II Hub Category 5 UTP or STP cable.

Cabling Requirements for 10/100 Bridge with the 10BASE-T/100BASE-TX Module

This module incorporates two RJ-45 connectors, one MDI-X port and one MDI port. The MDI-X port performs an internal crossover function that allows easy connection to other devices using standard straight-through cables. The MDI ports do not have the internal crossover function, permitting connection to devices having an internal crossover function using standard straight-through cables.

Note: To connect to 100BASE-TX networks, you can use only Category 5 cables.

Cabling Requirements for 10/100 Bridge with the 100BASE-FX Module

This module incorporates two SC-type connectors, one RX and one TX, and requires multimode fiber cable.

Adding and Replacing Units in the Stack

Stacking Rules

1. All managed hubs must be grouped together at the top of the stack.
2. Add new managed hubs only at the top of the stack.
3. Add new manageable hubs only at the bottom of the existing stack.

Notes:

1. In a single managed hub stack with Version 1.1 or later, the Backup Function must be disabled through the Management Capability Setup Menu on the BOOT ROM Console.
2. In a multiple managed hub stack with Version 1.1 or later, **all** of the managed hubs must have the Backup Function enabled as shown in Figure 2-11.

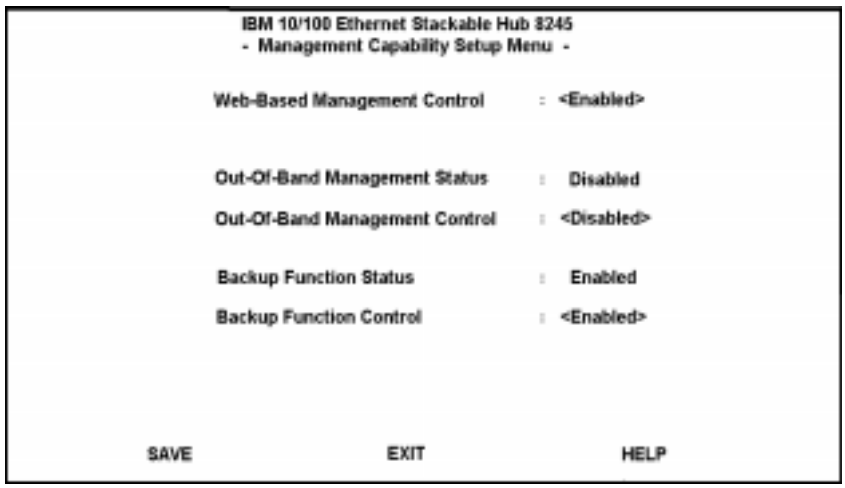


Figure 2-11 Disabling the Backup Function

Adding a Managed Hub Above An Existing Managed Hub

Step 1. Upload the existing configuration file to the TFTP server.

Step 2. If a managed hub with code earlier than Version 1.1 is being added to a stack, then the managed hub must first be upgraded to Version 1.1.

Step 3. Enable the Backup Function in the Management Capability Setup Menu of the BOOT ROM Console.

Step 4. Record the IP address, subnet mask, and default gateway of the current active managed hub. Assign a new IP address to the current active managed hub to eliminate a duplicate IP address when the configuration file is downloaded.

Step 5. Unpack the new managed hub and mount it into the rack above the existing active managed hub. This unit will become the new active managed hub. Do not connect the stack link cables yet.

Step 6. Power on the new hub and log in.

Step 7. Assign the IP address, subnet mask, and default gateway that you recorded in step 2 to the new active managed hub.

Step 8. Configure and cable the ports accordingly.

Step 9. Remove power to the new hub.

Step 10. Attach the stack link cable to the back of the new hub and the hub below it.

- The existing hubs perform a warm start because of the change in the hub's ID.
- The ID of the existing hubs in the stack will increment by 1. The current managed hub will have ID 2.

Step 11. Power on the new hub.

Step 12. Through a local console, log onto the new active managed hub.

Step 13. Go to the System Download Menu (Figure 4-38 on page 4-61) and specify the TFTP server address, check the box for the configuration file download, and specify the correct path/filename of the configuration file saved in step 1.

Step 14. In the System Restart menu (Figure 4-39 on page 4-63) in the System Utility Menu, execute a Cold Restart.

Step 15. Add workstations to the managed hub and configure the ports, if necessary.

Adding a Manageable Hub to the Bottom of an Existing Stack

Step 1. Unpack and mount the new manageable unit at the bottom of the stack.

Step 2. Attach the stack link cable between the new hub and the one above it.

Step 3. Power on the new hub. You can configure the newly added hub from the managed unit within 10 seconds.

Step 4. Log into the active managed hub and configure the new hub if necessary.

Replacing a Backup Managed Hub or Manageable Managed Hub

Step 1. Remove the defective hub and replace with a new hub. Do not connect the stack link cables yet.

Step 2. Power on the new hub.

Step 3. Using a local console, log into the new hub and assign an IP address, subnet mask, and default gateway.

Step 4. Enable the Backup Function in the Management Capability Setup Menu of the BOOT ROM Console.

Step 5. Power off the new hub.

Step 6. Connect the stack link cables to the new hub.

Step 7. Configure and cable the ports accordingly, see Figure 2-8 on page 2-10.

Removing a Hub from the Stack

To remove an Ethernet Stackable Hub from a stack, use the following procedure:

Step 1. Disconnect the stack link cable of the hub that you want to remove from the stack.

Step 2. Power off the hub and remove it from the stack.

Step 3. Reconnect the stack link cables of the hubs that are still in the stack.

Step 4. Check the managed unit to see if each hub in the stack is displayed. If not, either do a warm start on the managed unit or disconnect the power cord from any hub in the stack, and reconnect.

Note: In a multiple managed hub stack, all managed hubs must be placed at the top of the stack.

Warm Start After Hub ID Changes

The hub will do a **warm start** if its Hub ID has been changed. This enables the managed unit to synchronize the physical Hub ID with its database. The duration of the warm start sequence depends on the number of units in the stack. Normally, it takes less than 40 seconds for a 6-unit stack.

If the managed unit warm starts, then all the statistical information will be cleared. To minimize the impact to the whole stack, add a new manageable unit at the bottom of the stack. Thus the managed unit will not warm start and the statistical data will be kept.

The configuration data will be synchronized from the active managed unit to the backup managed unit during a warm start. The synchronization occurs automatically every 30 minutes while the system is up.

Cascading Ethernet Hubs

The best way to appreciate the benefit of stacking hubs is to examine the method of interconnection used by simpler Ethernet workgroup hubs, which interconnect by cascading. Cascaded hubs are in the same collision domain. Figure 2-12 shows four Ethernet workgroup hubs labeled A, B, C, and D. Hub B and Stack C are cascaded from Stack A. If you are using straight-through cables, you could attach one end from an MDI port on stack A to an MDI-X port on hub B, another cable from an MDI-X port on stack A to an MDI port on stack C, and so on. See Figure 2-12 for an example using straight-through cables. Crossover cables are needed for MDI-to-MDI and MDI-X-to-MDI-X connections.

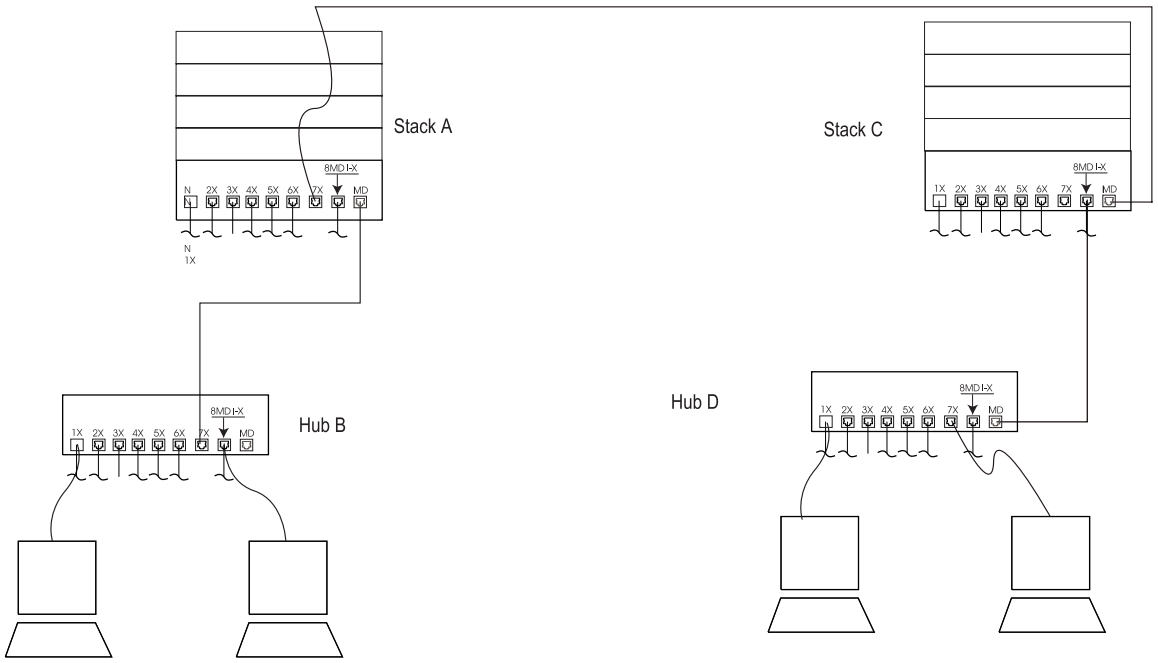


Figure 2-12 Cascading Ethernet Hubs

Because data sent from the workstation on Hub B passes through four hubs along the way to the workstations on Hub D, the workstation on Hub D is said to be four repeater hops from the workstation on Hub B. A repeater hop is counted whenever an Ethernet frame passes through a repeater. A stack of up to six 10/100 Ethernet Stackable Hubs is considered one hop.

Connecting Two Stacks of 10/100 Ethernet Stackable Hubs

10-Mbps Connections

If 10-Mbps connections are made between stacks, the IEEE 802.3 standard specifies that a frame sent from one workstation to another should not pass through more than four repeaters on the way to its destination and that there should be no more than five segments between any end devices in the same collision domain. Category 3, 4, or 5 cables can be used for 10-Mbps connections and the maximum length of each segment is 100 m (328 ft). Therefore, there can be up to 500 m (1640 ft) between end devices that have been cascaded at 10 Mbps. The 10-Mbps segments of the cascaded hubs are in the same collision domain.

Note: The 10/100 Ethernet Stackable Hub 8245 supports auto-negotiation. When connecting two stacks together, it will automatically link at 100 Mbps. To run at 10 Mbps, you will need to manually configure the ports to 10 Mbps.

100-Mbps Connections

If 100-Mbps connections are made between stacks, the IEEE 802.3u standard specifies that there can be only one repeater cascaded from another in the same collision domain. Only Category 5 cable can be used and it cannot be longer than 5 m (16 ft. 5 in.). Therefore, the maximum cable distance between end devices that have been cascaded at 100 Mbps is 205 m (672 ft). The 100-Mbps segments of the cascaded hubs are in the same collision domain.

External bridge Connections

The external bridge separates collision domains.

With TX module: If you connect the external 10BASE-T/100BASE-TX bridge module of one stack to an MDI or MDI-X port in another stack, no hops are counted. This connection can be 10-Mbps or 100-Mbps and can be up to 100 m (328 ft) in length.

With FX module: You can connect two stacks of 10/100 Ethernet Stackable Hubs with two 100BASE-FX bridge modules. The fiber distances can be 412 m (1352 ft) if half duplex and 2000 m (6560 ft) if full duplex.

Use TX/FX expansion modules to cascade unlimited number of 8245 hubs. This method will allow you to cascade unlimited numbers of 10/100 Ethernet Stackable Hubs.

With AUI expansion module: You can use the AUI expansion module to connect to 10BASE-T, 10BASE5, 10BASE2, or 10BASE-F network segments via the transceivers.

Chapter 3. Control Panel Management

The control panel is an effective management tool for monitoring and configuring the 10/100 Ethernet Stackable Hub 8245. It displays the following types of information:

- Port utilization
- Port statistics
- Port configuration
- Hub configuration

On the backup managed unit, the control panel shows only the port status and the control keys are used to switch between port groups.

Control Panel

The control panel shown in Figure 3-1 has the following features:

- Control Keys (MENU, SCROLL, and ENTER) - enables you to select menu items, make configuration settings, and navigate the menu structure.

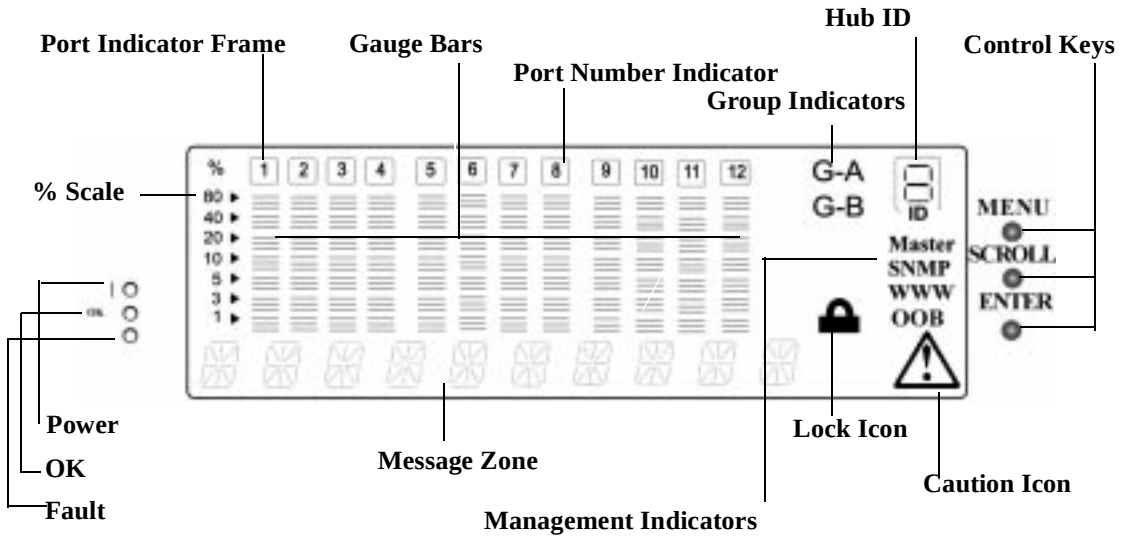


Figure 3-1 Control Panel

VFD Display

The vacuum fluorescent display (VFD) displays the following port and system information:

% Scale

The relative percentage of utilization or collision.

Port Number Indicators (1 to 12)

Port Number Indicators show the port number and with their brightness, indicate the status information. See Table 3-1.

Port Indicator Frame (☐)

The Port Indicator Frame indicates which ports are disabled. See Table 3-1.

Table 3-1 Port Information

Number	Frame	Indicates
Normal	Off	The port is available but the link is down.
Bright	Off	The port is available and the link is up.
Blinking	Off	The link is up and receiving data.
Bright	On	The port is disabled by the administrator.
Bright	Blinking	The port is auto-partitioned by the device.

Message Zone

Displays test messages, the menu items, and status information. If this managed unit is not the top managed unit in the stack (active managed unit), then it will display the backup managed unit's information in this area.

Gauge Bars

Displays information such as utilization or port status.

Lock Icon

Indicates that the control panel configuration is locked.

G-A

Displays status of ports 1 to 12 in Port Group A.

G-B

Displays status of ports 13 to 24 in Port Group B.

Master

Indicates that the hub is a managed hub.

SNMP

Indicates that the hub is SNMP-manageable.

WWW

Indicates that the Web Management feature is enabled.

OOB

Indicates that out-of-band is enabled.

CAUTION ICON

Indicates that an error has occurred.

Control Keys

You use the control keys to navigate through the menus and make selections. Table 3-2 indicates the function of each key.

Table 3-2 Control keys

Key	Action
MENU	Return to the previous level
SCROLL	Choose another topic within the same level
ENTER	Go to the next level or view status

Note: For a backup managed unit, you use the control keys only to switch the display of port status from Port Group A to Port Group B.

Power and Error Indicators

Power

Indicates that power is connected.

OK

Indicates that the self-diagnostic test was run without errors.

Fault

Indicates that the self-diagnostic test found an error.

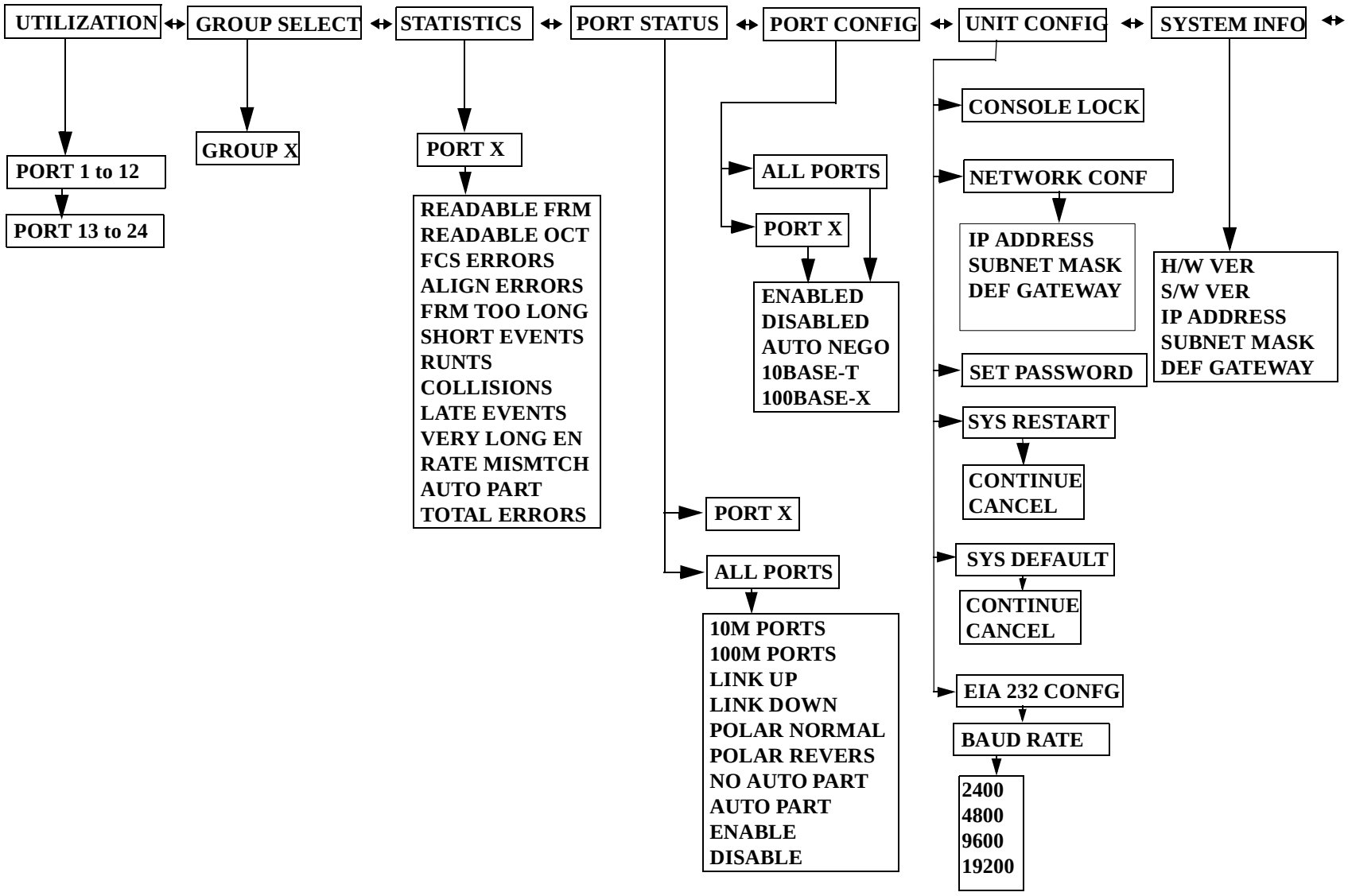
Table 3-3 Power and Error LEDs

LED	Position	State	Meaning
Power (green)	Top	On	The 10/100 Ethernet Stackable Hub 8245 power supply is good.
OK (green)	Middle	On	The hub is working correctly.
		Off	The hub is not working correctly.
Unlabeled (fault) (amber)	Bottom	On	A power-on failure has occurred.
		Off	The hub is working correctly.
		Blinking	Diagnostics are in progress.

Menu Structure

Figure 3-2 shows the control panel's menu structure.

Fig. 3-2 Menu Structure



Control Panel Inactivity

If you do not use the control keys for a period of 15 minutes, the control panel configuration is automatically locked and the VFD returns to utilization mode.

After an hour of inactivity, the VFD turns off. Pressing any control key reactivates the VFD.

Monitoring Network Utilization

You can observe the network traffic in the control panel by selecting the Utilization menu as shown in Figure 3-3. The utilization rate of each segment is represented by a bar graph consisting of 7 gauge bars. These shift continuously from left to right as time elapses, as shown in Figure 3-3 and Figure 3-4. In the message zone, the word UTILIZATION alternates periodically with the labels “10 M" "100 M.”

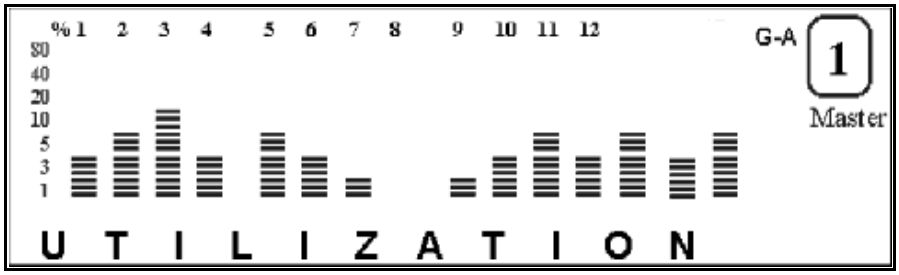


Figure 3-3 Utilization for 10-Mbps and 100-Mbps Segments

The 10-Mbps segment utilization is displayed on the left and the 100-Mbps segment utilization is displayed on the right.

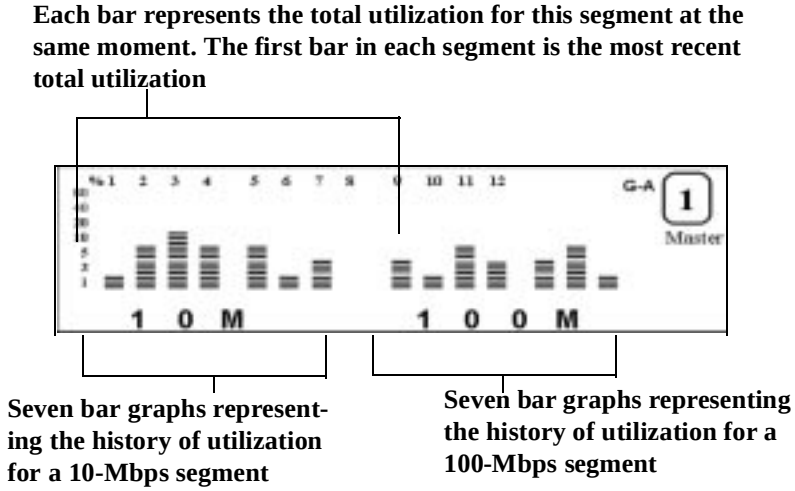


Figure 3-4 Utilization for 10-Mbps and 100-Mbps Segments

Selecting a Hub

In the hub selection main menu, **GROUP SELECT** is displayed in the message zone. The hub ID in the message zone is referred to as GROUP. The current hub ID is indicated by the “group cursor” (3 bar scales) under the port indicator as shown in Figure 3-5.

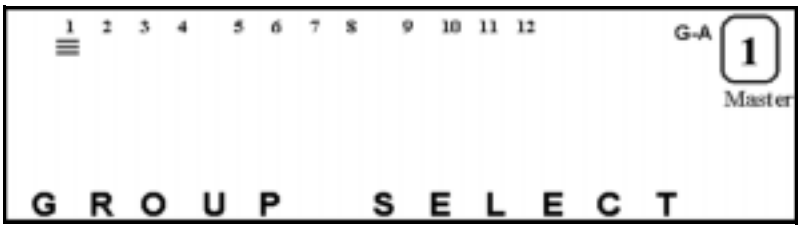


Figure 3-5 Group Select

Figure 3-6 illustrates that the current hub ID is 2, by the “group cursor” under port indicator 2 and by “GROUP 2” in the message zone.

Figure 3-6 Group 2

Monitoring Detailed Port Statistics

The statistics of each port for a selected hub can be monitored by selecting the Port Statistics menu. The current selected hub, for example, Hub 3, is indicated by the 3 bar scales under the port indicator number as shown in Figure 3-7.

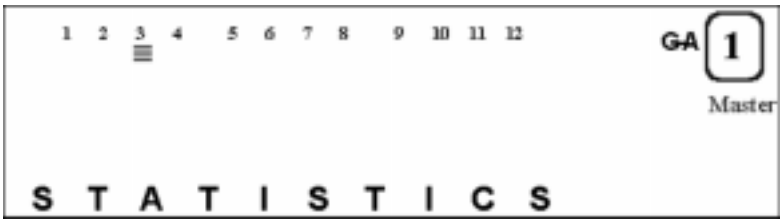


Figure 3-7 Statistics

Selecting a Port

Step 1. On the port statistics main menu, press **ENTER** to select a port for viewing its statistic counter.

Step 2. On the port selection menu, the current hub (Hub 3) is indicated by 3 bar scales under the port number indicator. The selected port number is displayed in the message zone, and 6 bar scales below the port number (port cursor) also indicates the current selected port as shown in Figure 3-8.

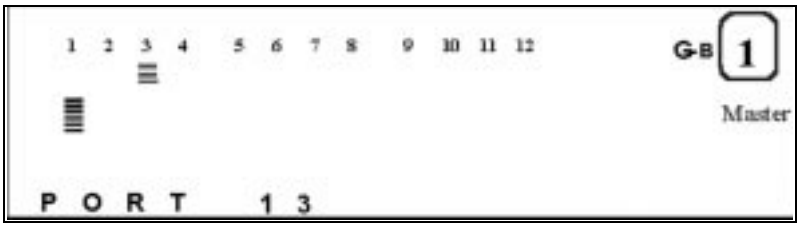


Figure 3-8 Port Select

Step 3. Press **SCROLL** to select the next port. The port cursor moves to the corresponding position under the port number indicator, and the corresponding port number is displayed in the message zone.

Step 4. Press **ENTER** to confirm the selection of the port and then go to the counter selection menu. The name of the port statistic counter is displayed in the message zone. Figure 3-9 shows the readable frame (READABLE FRM) statistic counter in the message zone for port 13 of hub 3.

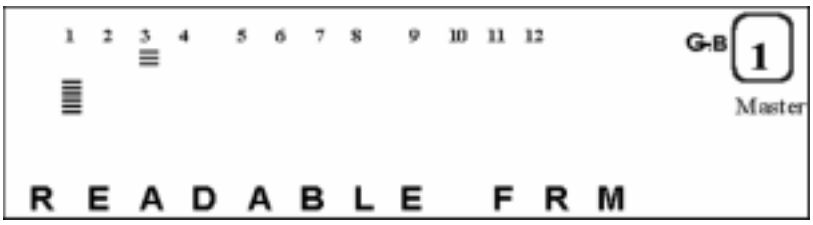


Figure 3-9 Readable Frame

Step 5. Press **SCROLL** to scroll through each type of counter.

Step 6. Press **ENTER** to view the value of the counter. The value of the counter is displayed in the message zone. Figure 3-10 shows the statistic counter, 1500 readable frames for port 13 of hub 3.

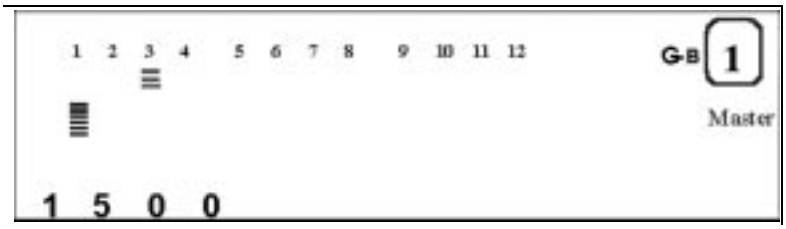


Figure 3-10 Statistic Counter Value

READABLE FRAMES

The total number of frames received on the hub port.

READABLE OCTETS

The total number of octets of data received on the hub port.

FCS ERRORS

The total number of packets received by the port that had a bad Frame Check Sequence.

ALIGN ERRORS

The total number of packets received that had bad FCS with a non-integral number of octets.

FRM TOO LONG

The total number of received packets that are longer than 1518 octets (including FCS octets but excluding framing bits) but are otherwise well formed.

SHORT EVENTS

The total number of received packets that are less than 64 octets (including FCS octets but excluding framing bits) and are otherwise well formed.

RUNTS

The total number of received packets that are less than 64 octets due to collisions or activity duration that is greater than the ShortEventMaxTime event and less than the ValidPacketMinTime event.

COLLISIONS

Total collisions.

LATE EVENTS

Total events received by the port where the activity duration is greater than the LateEventThreshold.

VERY LONG EVENTS

Total events received by the port where the activity duration is greater than the MAU Jabber Lockup Protection timer TW3.

RATE MISMATCH

Total frames received by the port with no collisions and the activity duration is greater than the ValidPacketMinTime event and also frequency (data rate) is detectably mismatched from the local frames mismatch frequency.

AUTO PART

Total number of times the port is auto-partitioned.

TOTAL ERRORS

Total errors received by the port including FCS errors, Align errors, Frame Too Long, Short Events, Late Events, Very Long Events and Rate Mismatch.

Monitoring Port Status Information

Monitor detailed port information by selecting the Port Status menu. Press **SCROLL** until PORT STATUS is displayed in the message zone. The currently selected hub is indicated by the group cursor under the port ID indicator as shown in Figure 3-11.

Figure 3-11 Port Status

Selecting Ports

You can view the status of all ports either in a single display or in a single port.

Single Port

To view the status of a single port:

Step 1. Press **ENTER** to go to the port selection menu. PORT X is displayed in the message zone and a bar graph is displayed under the port number as shown in Figure 3-12.

Step 2. Press **SCROLL** to select a port.

Step 3. Press **ENTER** to view port status. The port status scrolls automatically until you press any control key.

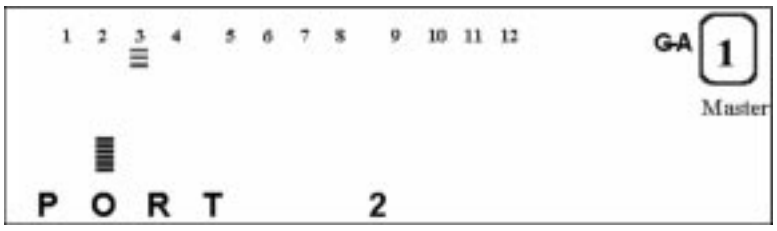


Figure 3-12 Individual Port Status

All Ports

To view the status of all ports:

Step 1. Press **ENTER** to go to the port selection menu.

Step 2. Press **SCROLL** to scroll to ALL PORTS. A bar graph under all the ports is displayed in the message zone. The top row of bars represents ports 13 to 24 and the bottom row represents ports 1 to 12.

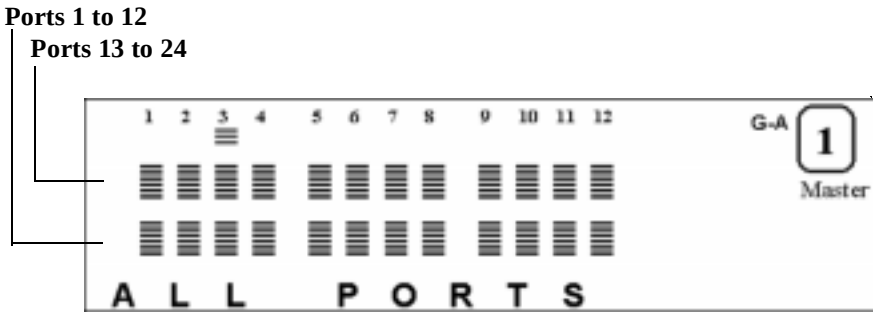


Figure 3-13 All ports

Step 3. Press **ENTER** to view all port statuses. A bar graph is displayed under each port number that is configured as shown in the message zone. Figure 3-14 shows the ports configured as 10-Mbps ports on hub 3.

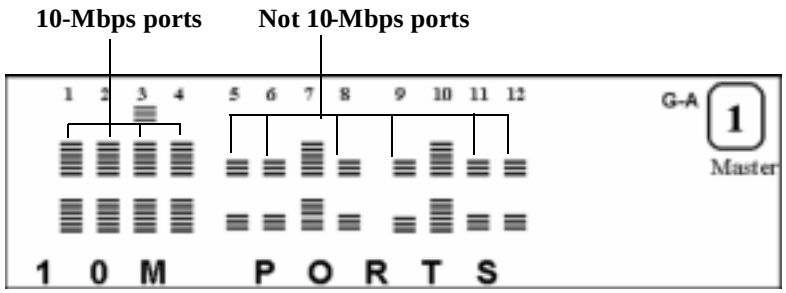


Figure 3-14 All 10-Mbps Ports

Step 4. The name of port status is displayed in the message zone. Press **SCROLL** to view the next status of all ports. Figure 3-15 shows the ports configured as 100-Mbps ports on hub 3.

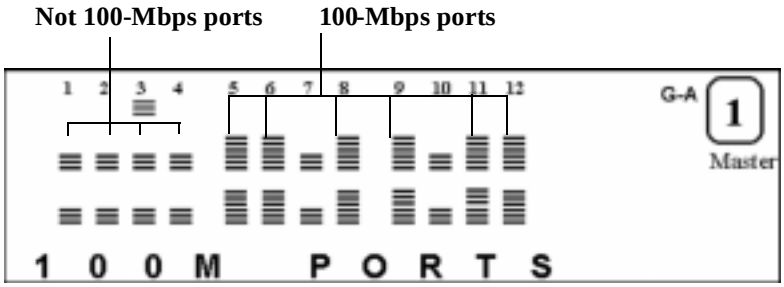


Figure 3-15 100-Mbps Port Status

Table 3-4 lists the possible status of ports.

Table 3-4 Port Status

10M PORTS	The port is set to 10-Mbps operation.
100M PORTS	The port is set to 100-Mbps operation.
LINK UP	The port is linked.
LINK DOWN	The port link is down.
POLAR NORMAL	The received (Rx) polarity of the port is normal.
POLAR REVERS	The received (Rx) polarity has been automatically crossed by the hub.
NO AUTO PART	The port is not auto-partitioned.
AUTO PART	The port is auto-partitioned.
ENABLE	The port is enabled.
DISABLE	The port is disabled.

Configuring Ports

The PORT CONFIG menu allows you to configure individual ports or all ports at one time. You are prompted to enter the password when the console is locked. You must configure the ports to match the devices at the other end of the link. Settings such as speed must be identical. Set all ports to AUTO NEGO as the default value. When you set the AUTO NEGO mode, the highest speed supported by both ends is negotiated by the port and the device at the other end.

In the Port Setting menu, PORT CONFIG is displayed in the message zone and the currently selected hub is indicated by the group cursor under the port number indicator as shown in Figure 3-16.

Figure 3-16 Port Configuration

Configuring All Ports

Step 1. Press **ENTER** to go to the port selection menu.

Step 2. Press **SCROLL** to select All PORTS.

Step 3. Press **ENTER**. The configuration is displayed in the message zone as shown in Figure 3-17.

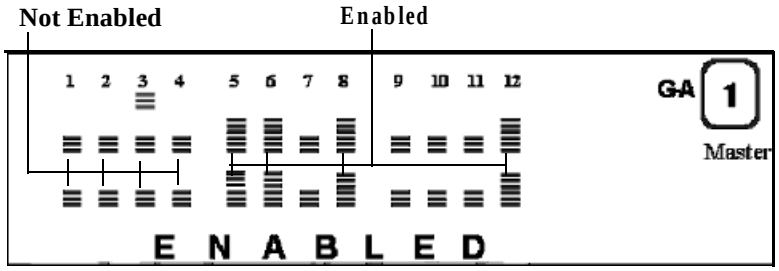


Figure 3-17 Current Port Configuration (All Ports)

Step 4. Press **SCROLL** to scroll through each configuration item.

Step 5. Press **ENTER** to apply the configuration to all ports.

Configuring Single Ports

Step 1. Press **ENTER** to go to the port selection menu.

Step 2. Press **SCROLL** to select a port.

Step 3. Press **ENTER**. The status of the port is displayed as shown in Figure 3-18.

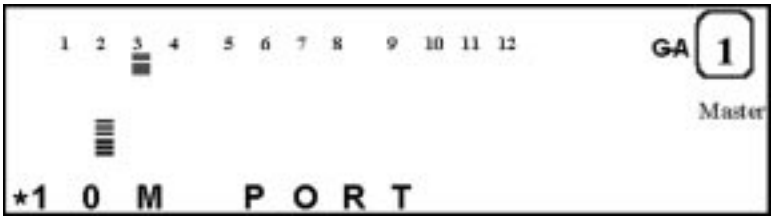


Figure 3-18 Current Configuration

Step 4. Press **SCROLL** to scroll through each configuration item.

Step 5. Press **ENTER** to apply the configuration to the port.

The applied configuration is indicated by an asterisk (*) displayed before the name of the configuration in the message zone as shown in Figure 3-18.

The following is a list of port configuration options:

- ENABLED
- DISABLED
- AUTO NEGO
- 10BASE-T
- 100BASE-X

Unit Configuration

The unit configuration menu allows you to configure the 10/100 Ethernet Stackable Hub 8245. When the device is locked, you are prompted for a password. How to enter the password entry is described in “Unlocking and Locking the Control Panel” on page 3-18.

To configure the unit:

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Enter the password (if the control panel is locked).

Step 3. Scroll to the appropriate menu item, press **ENTER**, and then follow the procedure for the selected item.

Figure 3-19 Unit Config Main Menu

Unlocking and Locking the Control Panel

Control panel security is maintained by the console lock menu. The lock icon is an amber lock symbol on the lower right of the VFD and is On when the control panel configuration is locked. When the control panel is unlocked, it automatically locks again after 15 minutes of inactivity. You must unlock the control panel to access the port configuration and unit configuration menus.

To unlock the control panel:

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Enter the password. The default password is 0000. The control panel is now unlocked.

To lock the control panel at any time:

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Scroll to CONSOLE LOCK and press **ENTER** twice. An asterisk (*) appears before LOCK.

Step 3. Press **MENU** to exit.

The control panel is locked as shown in Figure 3-20 and the lock icon appears in the control panel.

Figure 3-20 Control Panel Lock

Network Configuration

You can configure the hub IP address, subnet mask, and default gateway with the Network Configuration Menu.

IP address

The current IP address is displayed in the IP address configuration menu.

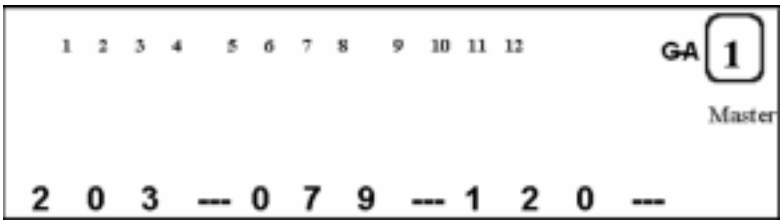


Figure 3-21 IP Address

To configure the IP address:

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Scroll to NETWORK CONF and press **ENTER.**

Step 3. Scroll to IP ADDRESS and press **ENTER**.

Step 4. Press **SCROLL** to increase the digit (0 to 9).

Step 5. Press **ENTER** to set the digit and move the cursor to the next digit. The current digit is blinking.

Step 6. The hub must be restarted for the configuration to take effect.

Because the message zone cannot contain the whole IP address, the IP address will shift left when the last digit in the message zone is set, as shown in Figure 3-22. When you complete the setting of the IP address, the system will validate the IP address. If the IP address is valid, the display will show the IP address, and system will apply the setting when the system is restarted. Otherwise, the system will reject it, and a message FAIL will be displayed for a few seconds. The invalid IP address is displayed again to allow you to modify it.

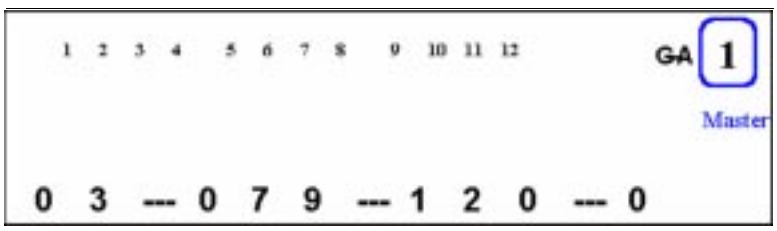


Figure 3-22 IP Address Shift Left

Subnet Mask

The subnet mask is displayed and configured in the same way as the IP address.

Default Gateway

The default gateway is displayed and configured in the same way as the IP address.

Securing the 10/100 Ethernet Stackable Hub 8245

The 10/100 Ethernet Stackable Hub 8245 is secured by automatically locking the control panel. A password must be entered to unlock the control panel before configurations can be made. You can configure a four-digit password. The default password is 0000.

Unlocking and Setting the Password

Step 1. Scroll to UNIT CONFIG and press **ENTER**. You are prompted to enter the password. **** PSW appears in the message zone and the first asterisk (*) flashes. Press **SCROLL** to increase the digit.

Step 2. Unlock the control panel by entering the default password 0000 one digit at a time by pressing **SCROLL** once and **ENTER** once to progress to the next digit.

Step 3. Repeat Step 2 three times. The control panel is unlocked.

Step 4. Scroll to SET PASSWORD and press **ENTER**.

Step 5. Enter a new password and press **ENTER**.

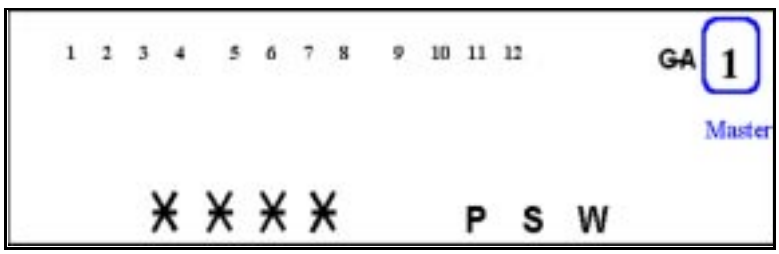


Figure 3-23 Set Password

Restarting the 10/100 Ethernet Stackable Hub 8245

You can restart the system by using the System Restart Menu. At this time, your configurations will be used to set up the system.

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Scroll to SYS RESTART and press **ENTER.**

Step 3. Press **ENTER** at CONTINUE or press **SCROLL** to end the action at the menu option CANCEL.

Step 4. Press **ENTER** to confirm.

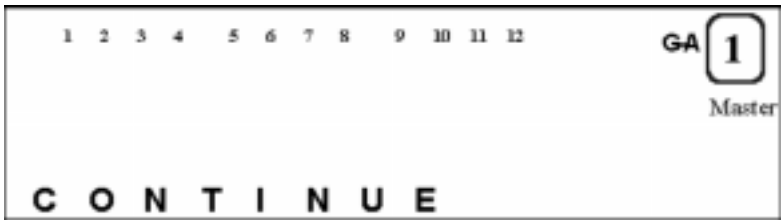


Figure 3-24 Continue

Restoring System Default Settings

Selecting the system default option resets all settings back to the factory default settings. All custom settings, including password, port configurations and unit configurations will be set to factory default settings.

Restore the system defaults with the following steps:

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Scroll to SYS DEFAULT and press **ENTER** to confirm.

Configuring the EIA 232 Port

You can configure the baud rate for SLIP connections. The default (9600) is indicated by an asterisk (*).

Step 1. Scroll to UNIT CONFIG and press **ENTER**.

Step 2. Scroll to EIA 232 CONFG and press **ENTER**.

Step 3. Scroll to BAUD RATE and press **ENTER**. Press **ENTER** again until an asterisk (*) appears in front of the selected baud rate. Press **MENU** to exit.

Baud Rates:

- 2400
- 4800
- 9600
- 19200

System Information

To view system information:

Scroll to **SYSTEM INFO** menu and press **ENTER**. The following system information is sequentially displayed until you press **MENU** or **SCROLL**.

- Hardware Version
- Software Version
- IP Address
- Subnet Mask
- Default Gateway

Chapter 4. Using the Management Interface

The 10/100 Ethernet Stackable Hub 8245 incorporates a powerful management interface that supports VT100 terminal emulation.

Note: With Software Version 1.10 and later, if a managed unit is operating in backup mode, it cannot go into runtime mode. When using the management interface you can see only the Boot ROM console. (See Chapter 6 for a more detailed description of the Boot ROM console).

Setting Up a Management Session

You can set up a management session by connecting a direct null-modem cable between the management port on the 10/100 Ethernet Stackable Hub 8245 and the communication port of your PC or terminal.

To connect a local terminal to the hub, perform the following steps:

Step 1. Install a terminal emulation application such as Windows® Hyperterminal on your PC.

Step 2. Configure the terminal emulation application as follows:

Baud rate	9600
Parity	None
Data bits	8
Stop bits	1
Flow control	None

Step 3. If you are using Microsoft® Windows terminal emulation, disable the “Use Function, Arrow, and Ctrl Keys for Windows” option in the Terminal Preferences menu under Settings.

Step 4. Connect the EIA 232 management port on the hub to your PC or DTE device using a null modem cable or straight-through cable and null-modem adapter. The 10/100 Ethernet Stackable Hub has a 9-pin, male connector. For more information, see “Connecting a PC to the Management Port” on page 2-13.

Step 5. Press **ENTER** 2 or 3 times and the login panel to the management interface appears.

Setting Up a Telnet Session

You can use any Telnet application that emulates VT100 terminal to establish an in-band session on the 10/100 Ethernet Stackable Hub 8245. Only one Telnet session can be active at a time. Before you can start a Telnet session, you must configure the IP parameters for the 10/100 Ethernet Stackable Hub 8245. Do this by using the Network Configuration Menu on the control panel or by using the serial management port. To open a Telnet session, you must specify the IP address assigned to the hub. For information on how to specify an IP address in your Telnet application, refer to your Telnet application documentation.

When the connection is established, the management interface login panel is displayed, as shown in Figure 4.3, “Login Panel,” on page 4-5

Note: Telnet is a component of most TCP/IP applications. You need to install TCP/IP on your workstation before you can use this interface.

Navigating the Management Session

Selecting Help on any panel displays the Help Menu shown in Figure 4-1.

Figure 4-1 Help Menu

This Help menu lists the additional keystroke functions.

Panel command usage:

- The commands available on each panel are displayed at the bottom of the panel.
- Use the Tab and Up and Down arrow keys to toggle through available commands. Use the left and right arrow keys to toggle through selections within a command. If brackets enclose a field on a panel, [*field*], you must type in the value of that field. If less-than and greater-than signs, <*field*> enclose a field on a panel, you can toggle a list of values with the toggle command, Ctrl+S.

Status and read-only fields are auto-refreshed every 5 seconds. Editable and input fields are not auto-refreshed but you can refresh them by pressing **F2**. Index fields, such as group number and port number are refreshed each time the cursor moves through the index field.

Menu Conventions

The menu conventions used in the management interface are shown in Figure 4-2.

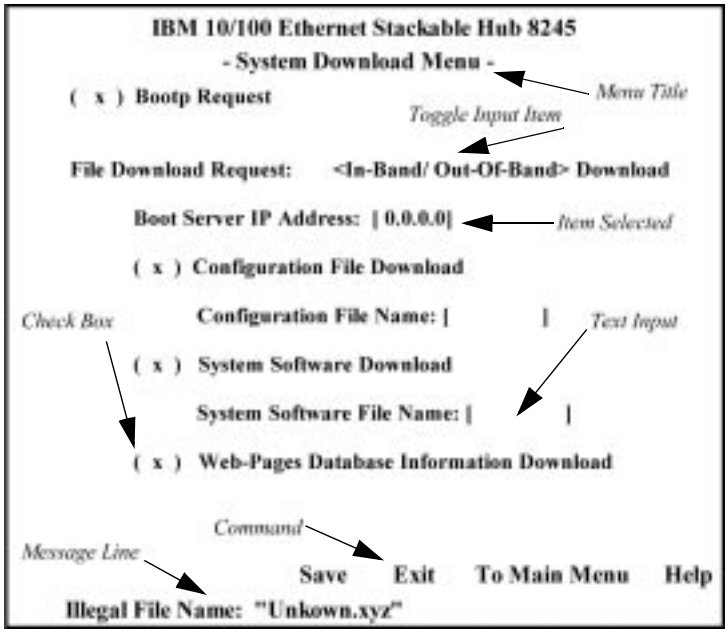


Figure 4-2 Menu Conventions

Menu Title

Describes the current configuration menu.

Toggle Input Item

Allows you to toggle the available options for items that appear between "< >" symbols. Toggle with Ctrl+S.

Item Selected

Highlight the current cursor location.

Check Box

Allows you to select or deselect items. Parentheses "( )" preceding an item denote a check box.

Text Input

Allows you to enter text from the keyboard. Highlighted items appearing between square brackets "[ ]" are text input fields that you can edit.

Message Line

Displays messages, usually error messages, indicating how to proceed.

Command

Displays the valid commands allowed in the current menu.

Note: The panel refreshes every few seconds. Only status fields will be refreshed.

Beginning a Management Session

The login panel, as shown in Figure 4-3, appears when you establish a connection between your terminal and the 10/100 Ethernet Stackable Hub 8245.

Note: If the terminal panel does not appear, press **Enter** two or three times.

Figure 4-3 Login Panel

To begin a console session, perform the following steps:

Step 1. Type your user name, if one has been configured. User names and passwords are ***not*** case-sensitive. The hub comes with two default user names. One default is “admin” and requires no password. The other default is “guest” and has a password of “guest.” Press **Enter**.

Step 2. Type the password, if one has been configured. There is no default password for a user name. Press **Enter** to advance to the Main Menu.

Main Menu

Selecting this option displays the Main Menu as shown in Figure 4-4.

Figure 4-4 Main Menu

System Information

Allows you to view general system information as well as specify location and contact information.

Management Setup

Allows you to view and specify management configurations.

Device Control

Allows you to monitor and configure hubs.

Network Monitor

Allows you to monitor statistic counters.

User Authentication

Allows you to configure user names and passwords.

System Utility

Allows you to configure software downloads, restart options, and Telnet session timeout intervals.

System Information

Selecting this option displays the System Information Menu as shown in Figure 4-5.

Figure 4-5 System Information Menu

The System Information Menu provides information related to the version of the system software installed on the hub.

You can specify up to 48 alphanumeric characters each for the System Name, Contact, and Location to provide useful information to all users concerning the 10/100 Ethernet Stackable Hub 8245. The information on this panel should be kept current so that persons requiring assistance know whom to contact.

Notes:

1. You must select **SAVE** to save any changes you have made.
2. The MIBs supported field is for information only.

System Description

A textual description of the entity. This also includes the name and version identification of the system's hardware type, software operating system, and networking software.

System Object ID

The vendor's authoritative identification of the network management subsystem is contained in the 10/100 Ethernet Stackable Hub 8245. This value is allocated within the SMI enterprises' subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of device is being managed.

System Manager

The management capability that this system supports (SNMP and WEB).

System Up Time

The time since the network management portion of the system was last restarted or powered on.

Management Setup

Selecting this option displays the Management Setup Menu shown in Figure 4-6.

Figure 4-6 Management Setup Menu

Network Configuration

Set IP address, Subnet Mask, Default Gateway, and SLIP address.

IPX Address Configuration

Set the IPX-address of device.

Serial Port Configuration

View and configure the management port.

SNMP Community

Configure community names and access right.

Trap Receiver

Set up community trap addresses.

IPX Trap Receiver

Set the locations to receive the SNMP traps for IPX.

Management Capability Setup

Enable or disable Web access and out-of-band management.

Trap Filter

Enable/disable trap filters.

Network Configuration

Selecting this option displays the Network Configuration Menu shown in Figure 4-7.

The Network Configuration Menu allows you to set up Ethernet and SLIP connections to the 10/100 Ethernet Stackable Hub 8245. Use Network Interface <1> to configure Ethernet connections and Network Interface <2> to configure SLIP.

Ethernet Configurations

An Ethernet connection allows you to monitor and configure the hub with a local console via a Telnet session, a Web browser or SNMP management. You need to configure the IP Address and Subnet Mask to work with your LAN settings before you can make an Ethernet connection.

Figure 4-7 Network Configuration Menu (Network Interface <1> Interface type: Ethernet)

IP Address

The dotted decimal address assigned to the hub.

Subnet Mask

The dotted decimal subnet mask assigned to the hub.

Default Gateway

The dotted decimal IP address of the default gateway assigned to the hub.

The 10/100 Ethernet Stackable Hub 8245 must be restarted before the IP address, subnet mask, and default gateway can take effect. To ensure that the new information is correct, do a ping from another device that is connected to the hub.

Note: The hub does not respond to ping packets that are greater than 1484 bytes.

Slip Configuration

Slip connections enable monitoring and configuring the hub remotely with a modem.

Figure 4-8 Network Configuration Menu (Network Interface <2> Interface type: SLIP)

The baud rate, character size, parity, and stop bits are read only and not configurable on this menu.

Baud Rate

The current serial port baud rate that can be configured from the Serial Port Configuration Menu.

Character Size

8 bits.

Parity

None.

Stop Bits

1 stop bit.

IP Address

The dotted decimal address assigned to the SLIP interface of the hub.

Subnet Mask

The dotted decimal mask assigned to the SLIP interface of the hub management port.

IPX Address Configuration

Selecting this option displays the IPX Address Configuration Menus as shown in Figure 4-9.

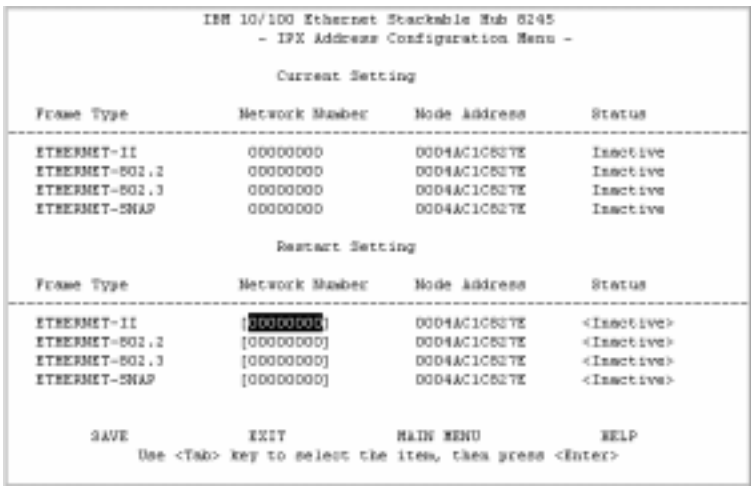


Figure 4-9 IPX Address Configuration Menu

Use this menu to set the IPX-address of each device. There are two parts provided in the menu. Current Setting (Read Only) is the configuration currently applied to the IPX module that was read from a Novell server when the hub was last started. Restart Setting (Read/Write) is the setting that will be applied when the system restarts without connecting to any Novell server.

Frame Type

Each frame type corresponds to one network interface. Select the data link protocol used from among these four available protocols:

- Ethernet-II
- Ethernet-802.2
- Ethernet-802.3
- Ethernet-SNAP

Network Number

There is a network number for each frame type. When the system is restarted, it learns this automatically from the IPX router. If there is no IPX router to supply this information, the default setting will be applied. If the default setting is zero, the agent will self-configure with a unique number as its network number.

Node Address

This field is always the same as the device's MAC address.

Status

You can make certain frame types active or inactive to control the devices. Making a frame active allows its associated frame type to access it. Making a frame inactive will close the associated frame type.

Select **SAVE** to retain the new configuration. The hub must be restarted before the new configuration takes effect.

Note: If a new Novell server is attached to the network, a warm start must be issued for the hub for it to learn the network numbers from the new server.

Serial Port Configuration

Selecting this option displays the Serial Port Configuration Menu as shown in Figure 4-10 and Figure 4-11 on page 4-16.

The management port must be configured as shown in Figure 4-10 to connect a PC to the 10/100 Ethernet Stackable Hub 8245.

Console

The **CONSOLE** mode is used to view the configurations required to make a VT100 terminal emulator connection to the 10/100 Ethernet Stackable Hub 8245.

Figure 4-10 Serial Port (Console)

Note: The information displayed on the Serial Port Configuration Menu is read only.

Out-of-Band

The **OUT-OF-BAND** mode enables you to set up serial port configurations for making a connection to the 10/100 Ethernet Stackable Hub 8245 management port using a modem.

Figure 4-11 Serial Port (Out-of-Band)

Baud Rate

The baud rate can be configured as 2400, 4800, 9600, or 19200 bps. The default is 9600.

Character Size

8 bits.

Parity

No parity.

Stop Bits

1 stop bit.

Select **SAVE** to retain the new configuration. The new configuration takes effect if out-of-band management is enabled.

When SLIP is enabled, the EIA 232 port can be used for SLIP only. The EIA 232 port cannot be used to gain access to a management session via VT100 terminal emulation. If the SLIP connection is malfunctioning, you can disable SLIP by rebooting and pressing Enter when the Abort message appears. The message will appear for only 10 seconds. Also, OOB will appear on the lower right-hand side of the control panel when out-of-band management is enabled.

SNMP Community Setup

From the SNMP Community Menu, Figure 4-12, you can manage all aspects of SNMP communities. You can add, delete, or edit SNMP community names, set the access rights and alter the community state. Community names are *case sensitive*. For example, **Private** and **private** are considered different. You cannot enter the same name more than once. If you do, an error message will appear at the bottom of the screen. You can clear the error by pressing the **Esc** key.

Figure 4-12 SNMP Community Menu

This menu lets you assign up to six SNMP communities.

Community Name

Text string of up to 16 characters.

Access Right

Read Only: The SNMP manager can only view the status of the hub.

Read/Write: The SNMP manager can view and configure the hub.

Status

Enable: Enable the SNMP Community.

Disable: Disable the SNMP Community.

To add a community name:

Step 1. Highlight an index number and press **Enter.** An editable panel is presented as shown in Figure 4-13.

Step 2. Enter a name in the Input field.

Step 3. Set the Access Right and Status.

Step 4. Highlight **ADD** and press **Enter**. The new name is displayed.

Figure 4-13 SNMP Community Menu -2

To edit a community name:

Step 1. Highlight an index number with an existing community name and press **Enter.**

Step 2. Change the Access Right and Status.

Step 3. Highlight **Update** and press **Enter**.

To delete a community name:

Step 1. Highlight an index number with an existing community name and press **Enter.**

Step 2. Highlight **Delete** and press **Enter**.

Trap Receiver

Selecting this option displays the Trap Receiver Menu shown in Figure 4-14.

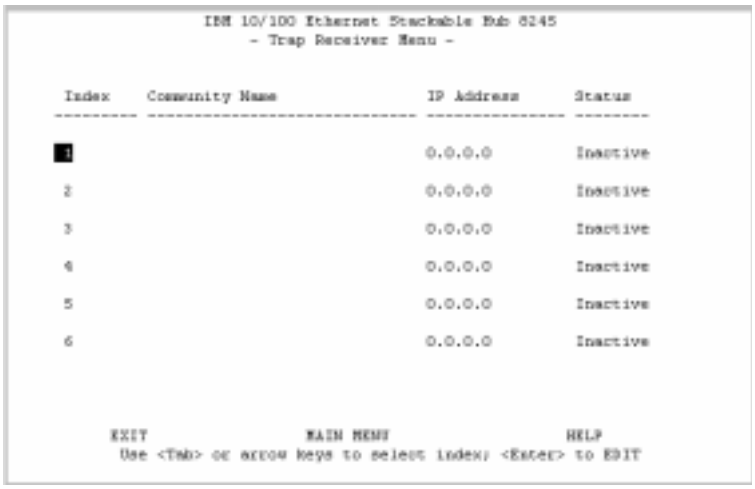


Figure 4-14 Trap Receiver Menu

Traps are messages sent across a network to an SNMP Network Manager. These messages alert the manager to changes in the hub. You can set up to six trap receivers.

Index

A number to identify a trap receiver (1 to 6).

Community Name

The authorized SNMP community string of the remote network manager (maximum 16 characters).

IP Address

The IP Address of the remote network manager station to which traps should be sent.

Status

A trap receiver's status can be either active or inactive. Trap receivers with active status receive all traps sent by the hub.

To set up trap receivers:

Step 1. Use the tab or arrow keys to select an index entry. Press **Enter** to edit or set up a trap receiver.

Step 2. Enter the **Community Name, IP address,** and **Status**.

Step 3. Select **UPDATE**.

Step 4. Repeat steps 1 through 3 for each new trap receiver.

Figure 4-15 Update Trap Receiver Menu

IPX Trap Receiver

Selecting this option displays the IPX Address Configuration Menu on Figure 4-16.

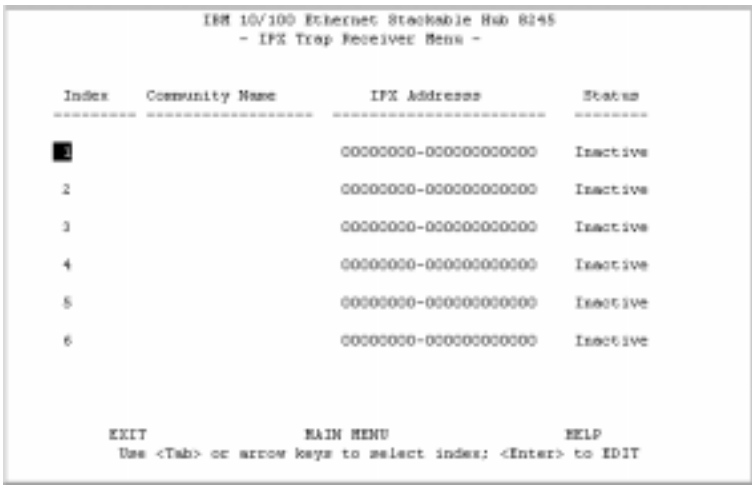


Figure 4-16 IPX Trap Receiver Menu

This function is similar to the Trap Receiver for IP Network. This menu is used to configure the Trap Receiver through the IPX network. You can set up to 6 IPX Trap Receivers.

Index

A number to identify a trap receiver (1 to 6).

Community Name

The authorized SNMP community string of the remote network manager (maximum of 16 characters).

IPX Address

The trap PDU destination consisting of two parts: the network number and node address. Only hexadecimal digits (0 through 9, A through F) can be used.

Status

A trap receiver's status can be either active or inactive. Trap receivers with active status receive all traps sent by the hub.

To set up trap receivers:

Step 1. Use the tab or arrow keys to select an index entry. Press **Enter** to edit or set up a trap receiver.

Step 2. Enter the **Community Name, IPX address,** and **Status**.

Step 3. Select **UPDATE**.

Step 4. Repeat steps 1 through 3 for each new trap receiver.

Figure 4-17 Update IPX Trap Receiver

Management Capability Setup

Selecting this option displays the Management Capability Setup Menu as shown in Figure 4-18.

Figure 4-18 Management Capability Setup Menu

This menu lets you enable or disable Web-based management and out-of-band management.

Web-Based Management

Enables or disables Web-based management. The new configuration takes effect after you execute **SAVE**.

Out-Of-Band Management Status

Displays the current status.

Out-Of-Band Management Control

Enables or disables out-of-band management (SLIP).

- When connecting with local serial port, the setting takes effect immediately.
- When connecting with Telnet, the system must be restarted before the setting takes effect.
- The default value is Disable.

Trap Filter

Selecting this option displays the Trap Filter Menu as shown in Figure 4-19.

Figure 4-19 Trap Filter Menu

This menu lets you enable or disable trap filters for those traps defined by RFC1215 and RFC1516. Selecting a trap filter disables the trap and no traps are sent for the specified condition. The default is all traps enabled.

Device Control

Selecting this option displays the Device Control Menu as shown in Figure 4-20.

Figure 4-20 Device Control Menu

This menu lets you configure each hub in the stack.

Repeater Group Control/Status
View and configure hubs.

Repeater Port Control/Status
View and configure hub ports.

Bridge Module Control/Status
View and configure bridge modules.

External AUI Module Control/Status
View and configure the external AUI module.

Redundant Link Control
Configure redundant link pairs.

Security Intrusion
Configure hub security.

Repeater Group Control/Status

Selecting this option displays the Repeater Group Control/Status Menu as shown in Figure 4-21.

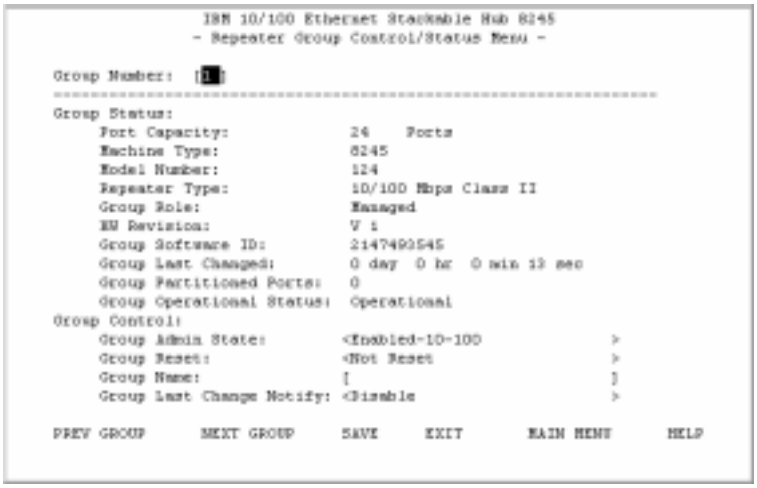


Figure 4-21 Repeater Group Control/Status

The Repeater Group Control/Status displays the status of hubs and allows you to enable or disable a hub as well as to name and reset it.

Group Number

The 10/100 Ethernet Stackable Hub ID assigned to the hub in the stack (1 to 6).

Port Capacity

The maximum number of ports that can be contained within the group.

Machine Type

Identifies the machine type (8245).

Model Number

The model number of the hub (012, 024, 112 or 124).

Repeater Type

The repeater type of the group (10/100-Mbps Class II).

Group Role

Active Managed Unit

The managed device having the lowest hub ID in the stack becomes the active managed unit. The active managed unit provides a complete set of the functions provided by the system. It must be the top unit in the stack.

Backup Managed Unit

The managed device having the second lowest hub ID in the stack becomes the backup managed unit. The backup managed unit is simply acting as a backup for the managed one. A duplication of the configuration occurs every 30 minutes, as well as when the active managed unit is restarted.

Manageable Unit

The manageable units are models 012 and 024 or managed units in the stack below the backup managed unit.

HW Revision

The hardware version of the 10/100 Ethernet Stackable Hub.

Group Software ID

The software ID number of the hub.

Group Last Changed

The value of system up time since any of the following conditions occurred:

- When a hub was connected or removed from the stack
- When a hub was restarted
- When a group was created (such as when a device or module was added to the system)
- When a change occurred in the value of hub operational status
- When ports were added or removed as members of the group (such as group admin enabled or disabled)
- When any of the counters associated with this hub were reset

Group Partitioned Ports

The total number of partitioned ports in the group.

Group Operational Status

Operational: The hub is connected to the stack and is functional.

Not Present: The hub is not present or not functioning.

Group Admin State

Enable or disable the specific group segment. The default value is Enabled Both 10-Mbps and 100-Mbps Admin only.

Enabled-10

Only the 10-Mbps segment of a given group is connected to the backplane of the stack. The 100-Mbps segment of a given group is isolated from the stack.

Enabled-100

Only the 100-Mbps segment of a given group is connected to the backplane of the stack. The 10-Mbps segment of a given group is isolated from the stack.

Enabled-10-100

Both 10-Mbps and 100-Mbps segments of a given group are connected to the backplane of the stack.

Disabled-10-100

Both 10-Mbps and 100-Mbps segments of a given group are isolated from the stack.

Group Reset

You can change all, some, or none of the group's function by selecting one of these options:

Note: The selected option takes effect after you select **SAVE**.

Not Reset

None of these will be reset.

Reset ALL

The function logic, counters, and repeater configuration of group will be reset. This is identical to cold restart.

Reset Function Logic Only

The function logic of group will be reset. The counters and repeater configuration will be held static and will not be reset. This reset operation will reset the link status of each port to ‘Link Down,’ which will cause a Link Status Change event to be raised.

Reset Counters Only

The counters of each port will be reset to 0, but the function logic and repeater configuration will be held static and will not be reset.

Group Name

The name assigned to this hub (up to 28 characters). It cannot be accessed by the SNMP Manager.

Group Last Change Notify

Enable

Sends out a trap when a setting in the Repeater Group Control changes.

Disable

Does not send out a trap when the setting in the Repeater Group Control changes.

To change the settings of a given group:

Step 1. Select the group by number.

Step 2. Set new value to Group Admin State.

Step 3. Set reset request to Group Reset field.

Step 4. Type in the name to the Group Name field.

Step 5. Set Group Last Change Notify field.

Step 6. Select **SAVE**.

Repeater Port Control/Status

Selecting this option displays the Repeater Port Control/Status as shown in Figure 4-22.

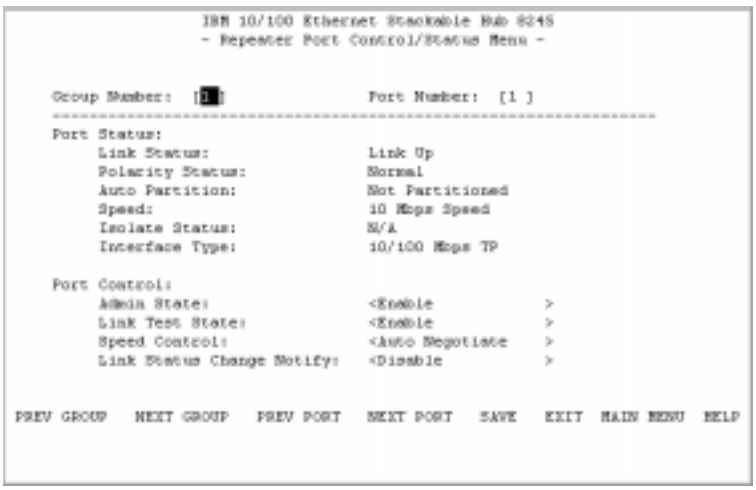


Figure 4-22 Repeater Port Control/Status

The Repeater Port Control/Status menu provides information about a hub's port status. A hub can be selected with the PREV GROUP and NEXT GROUP commands and its ports with the PREV PORT and NEXT PORT commands. The selected port state can be configured.

Group Number

The Ethernet Stackable Hub ID assigned to the hub in the stack (1 to 6).

Port Number

The port number of the hub specified in the Group Number.

Link Status

The current link status of the port.

Link Down: Link pulses are not detected on this port.

Link Up: Link pulses are being received on this port.

Note: When the port link test function is disabled, the Port Link Status always returns Link Up for ports.

Polarity Status

The current polarity link status of the port.

Normal: The receive polarity of the given port is not reversed.

Reversed: The receive polarity of the given port is reversed and has been automatically crossed by the repeater.

Auto-Partition

The current partition status of the port.

Not Partitioned: The port is not partitioned.
Partitioned: The port is partitioned.

Speed

The current speed of the port (10 Mbps/100 Mbps).

Isolate Status (100-Mbps Port Only)

Indicates whether this 100-Mbps port is currently isolated by the repeater.

- Not Isolated: The port is not isolated
- Isolated: The port is isolated.

Interface Type

The interface type of the port (10/100-Mbps TP).

Admin State

The current administration state of the port (enabled/disabled).

Link Test

Enable or disable link testing.

Note: Redundant link pairs must have Link Test enabled.

Speed Control

The port speed. The port will automatically connect to the 10-Mbps or 100-Mbps segment based on its port speed.

Auto Negotiate: The speed is detected and the duplex mode is forced to half duplex.
Force 10 - TP: The port speed is forced to 10 Mbps.
Force 100 - TP: The port speed is forced to 100 Mbps.

Link Status Change Notify

Enable: The trap is sent.

Disable: The trap is not sent.

Note: Whenever the Port Link Status is changed, the “hubPortLinkStsChgTrap” will be raised by the agent.

Bridge Module Control/Status

Selecting this option displays the Bridge Module Control/Status Menu as shown in Figure 4-23.

Figure 4-23 Bridge Module Control/Status Menu

Group Number

The hub ID number assigned to the 10/100 Ethernet Stackable Hub (1 to 6).

Bridge Module Status

Bridge Description

The characteristics of this bridge module:

- 10/100 Bridge with 10/100-TX Uplink
- 10/100 Bridge with 100 BASE-FX Uplink

Bridge External Port Interface Type

The interface type of external port for a given bridge module:

- TP port with RJ-45 interface
- Multi-Mode with SC type interface

External Port Link Status

The current link status of the installed module. This value is read-only.

- Link Up
- Link Down

External Port Speed

The module's external port speed. This value is read-only.

- Half Duplex 10 Mbps
- Full Duplex 10 Mbps
- Half Duplex 100 Mbps
- Full Duplex 100 Mbps

Hardware Status

The operation status of this bridge module.

Operate as Internal Plus External Bridge:

The internal bridge function and the external bridge function are enabled.

Operate as External Bridge Only:

The internal bridge function of a given bridge module is disabled via the hardware configuration.

Not Present:

There is no bridge module installed in the given group.

Bridge Module Control

External Function Admin State

Enable:

Enables the external bridge function.

Disable:

Disables the external bridge function of a given bridge. Once the external bridge function is disabled, you must enable it to restore external bridge operation.

The default value is Disable.

Internal Function Admin State

Enable:

Enables the internal bridge function. The internal hardware DIP switch must also be enabled for the internal bridge to function.

Notes:

1. The internal bridge must be enabled in hardware with the DIP switch settings before the Admin state can be enabled. See Figure 2-4 on page 2-8 and Figure 2-5 on page 2-8.
2. If you have a stack of all manageable units (no managed units), you only need to set the bridge module's hardware DIP switch to enable it to act as an internal bridge.

Disable:

Disables the internal bridge function when the internal hardware DIP switches have been enabled. Once the internal bridge function is disabled, you must enable it to restore internal bridge operation.

The default value is Disable.

Notes:

1. These modules are not hot-swappable. You must remove power from the 8245 before installing or removing bridge modules.
2. You should enable the internal bridge on only one bridge module when you have multiple bridge modules installed in a stack. This prevents a network loop condition.

External Port Link Status Change Notify

If enabled a trap will be sent to the receiver when link status of the port has changed.

Enable: The trap is sent to the trap receivers.
Disable: No trap is sent.

External AUI Module Control / Status

Selecting this option displays the External AUI Module Control/Status Menu as shown in Figure 4-24.

Figure 4-24 External AUI Module Control / Status Menu

The external AUI module is used to connect AUI devices to the 10/100 Ethernet Stackable Hub 8245. The AUI module is an external bridge and does not have an internal 10/100 bridge.

Group Number

A 10/100 Ethernet Stackable Hub ID in the stack (1 to 6).

Admin State

You can set this object to enable/disable the AUI port operation. If the AUI module does not exist, it will show <N/A>.

Redundant Link Control

Selecting this option displays the Redundant Link Control Menu as shown in Figure 4-25.

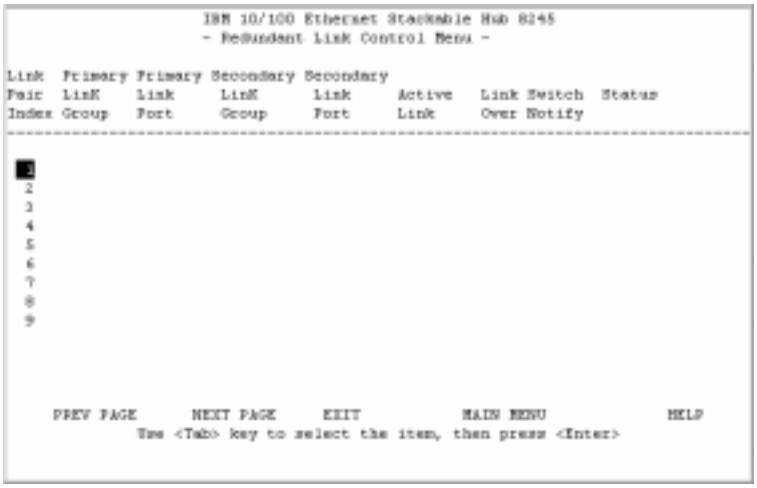


Figure 4-25 Redundant Link Control Menu

The Redundant Link Control Menu allows you to configure up to 18 pairs of redundant links. A redundant pair consists of any two physically linked ports in the 10/100 Ethernet Stackable Hub stack, where one is the primary link port and the other is the secondary link port. The primary link is the *active* link between two devices and the secondary is a backup and is set to *inactive* to prevent looping. If the primary link fails, the secondary link becomes active. The secondary link stays active even if the primary link recovers. You must manually reset the primary link status to active in order to reinstate the redundant pair.

You configure a primary link by assigning a specific port on a specific hub to a Link Pair Index. You assign a secondary link by assigning a specific port on a specific hub to the same Link Pair Index.

Link Pair Index

The number identifying the redundant link pair (1 to 18).

Primary Link Group

This object identifies the hub ID of the primary link for a given redundant link pair.

Primary Link Port

This object identifies the port number of the primary link for a given redundant link pair.

Secondary Link Group

This object identifies the hub ID of the secondary link for a given redundant link pair.

Secondary Link Port

This object identifies the port number of the secondary link for a given redundant link pair.

Active Link

This object indicates the current status for a given redundant link pair.

Primary: The primary port is currently the active link.

Secondary: The secondary port is currently the active link.

Both fail: Both the primary and secondary links have failed.

Link Switch Over Notify

If the link status of active link is down for more than 5 seconds then the *active link failed* is detected, port switchover is performed, and a trap is sent to the trap receivers.

Enable: A trap is sent to the trap receivers if a switchover occurs.
Disable: No trap is sent to the trap receivers if a switchover occurs.

Status

You can enable, disable, or suspend the operation of specific redundant link pairs.

Enable

The redundant link pair is in the normal operation mode. The primary port is active and the secondary port is disabled.

Disable

If you disable the primary port from the port control/status menu, the status of this link pair is changed to the *suspend state.* This indicates that the active port has been disabled and the redundant link function is temporarily suspended. If you enable the primary port later on, the status of this redundant link pair is changed to *enabled.*

If you disable the secondary port, the status of this link pair is changed to the *suspend* state and both ports are disabled. If you enable the secondary port later, the status of this link pair is changed to enabled and the redundant link pair is in the normal operation mode.

Notes:

1. Setting the redundant link to disable does not cause the ports to be switched over.
2. Redundant link pairs must have Link Test enabled.

Suspend

Indicates that the active ports are disabled and the redundant link function is temporarily suspended until you set its state to *enabled*.

Note: The suspend state does not cause the port to be switched over.

Invalid

Purge the configuration of a redundant link pair from the system database.

Return-to-primary

Selecting this option and pressing **Enter** reassigns the primary link as an active link again. A trap is sent to the trap receivers if the status of the redundant link is *enabled*. If the status is *suspend* then the link pair is reactivated but no trap is sent.

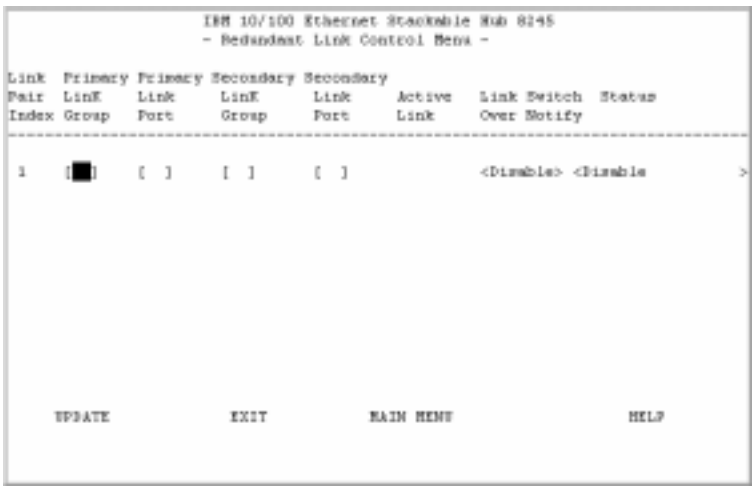


Figure 4-26 Redundant Link Control Menu

Configuring Link Pairs

Selecting this option displays the Redundant Link Control Menu as shown in Figure 4-26

Step 1. Select a link pair (1 to 18). Use NEXT PAGE to select pairs 10 through 18.

Note: You must enter at least one link pair on the FIRST PAGE in order to go to the NEXT PAGE.

Step 2. Enter the Primary Link Group (1 to 6).

Step 3. Enter the Primary Link Port (1 to 12/24).

Step 4. Enter the Secondary Link Group (1 to 6).

Note: You can configure and save the Secondary Link Group and the Primary Link Group as the same hub. However, this will be of no use in the event of a hub failure.

Step 5. Enter the Secondary Link Port (1 to 12/24).

Step 6. Enable the Link Switch Over Notify (optional).

Step 7. Enable the Status.

Step 8. Select **SAVE** to update the new linked pair. Repeat these steps for each link pair.

Editing a Link Pair

To edit a link pair, enter the link pair number of an existing link pair, reconfigure the rest of the columns, and then select **SAVE**. The link pair is updated to the new settings.

Deleting a Link Pair

To delete a link pair, enter the link pair number of an existing link pair, set the Status to invalid, and then select **SAVE**. The link pair is removed.

Security Intrusion Control/Status

Selecting this option displays the Security Intrusion Control/Status Menu as shown in Figure 4-27.

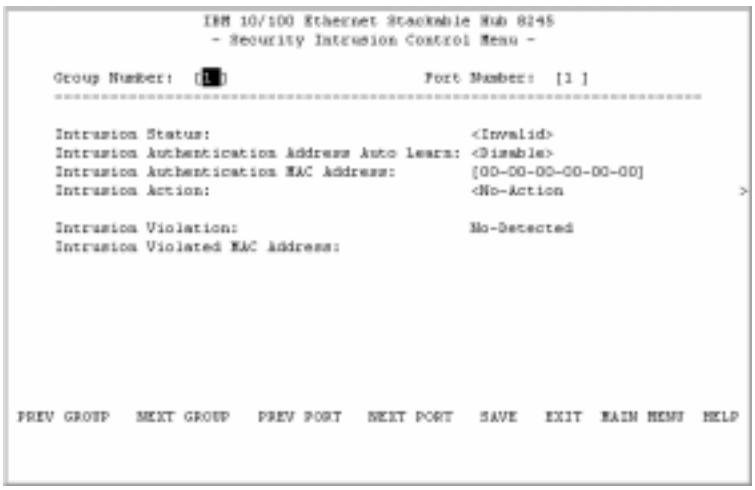


Figure 4-27 Security Intrusion Control/Status Menu

The intrusion control enables you to set up secure ports that allow access by a single authorized MAC address.

Group Number

The hub ID number that is assigned to the 10/100 Ethernet Stackable Hub 8245 (1 to 6).

Port Number

The port number of the hub that is specified in the Group Number (1 to 12/24).

Intrusion Status

Enable: Enable the security intrusion control for the current port.
Disable: The security intrusion control of a given port is disabled.
Invalid: Purge the security intrusion control configuration for the current port from the system database.

Intrusion Authentication Address Auto-Learn

Enable: The hub learns the MAC address of the first device that this port receives data from. After learning the MAC address the auto-learn function is disabled and the recorded MAC address is the authorized MAC address. This address is displayed in the Intrusion Authentication MAC address field.
Disable: Auto-learn operation is disabled.

Intrusion Authentication MAC Address

The MAC address of a device that is allowed to connect to this particular port.

Intrusion Action

The action that is performed when the hub detects an intrusion of an unauthorized MAC address.

No Action: No action will be taken.
Send Trap: A trap is sent to the trap receivers.
Partition Port: The port is partitioned.
Send-Trap-and-Partition Port: The port is partitioned and a trap is sent to the trap receivers.

Intrusion Violation

Detected: The MAC address that caused the intrusion is written to the Intrusion Violated MAC Address field.
Not-Detected: No intrusion has been detected.

Intrusion Violated MAC Address

Displays the MAC address of the last unauthorized device to send to this port.

Notes:

1. If another hub or unrouted switch is attached to a port with Security Intrusion enabled, then only one of possibly many MAC addresses will be allowed to pass data.
2. When you use the up arrow key to go from Port Number to Group Number, any data previously changed prior to saving will be reset to its previous state.

Network Monitor

Selecting this option displays the Network Monitor Menu as shown in Figure 4-28.

Figure 4-28 Network Monitor Menu

This menu lets you monitor the network traffic and analyze the network utilization.

Repeater Statistics Information

Hub statistics such as TX collisions, total frames, total errors, and total octets for both 10-Mbps segments and 100-Mbps segments.

Repeater Group Statistics Information

Displays statistics counters for each hub.

Repeater Port Statistics Information

Displays statistics counters for each port.

Address Tracking Information

Provides a way for a network management application to passively gather information about which network addresses are connected to which ports of a hub.

Address Search Information

Active address tracking capability is used to watch for a given MAC address and report which port it was seen on.

Broadcast Storm Protection

Monitors the broadcast counters of each hub port to detect if the broadcast storming exists in the network.

Broadcast Storm Detected

Each hub port or optional module port which causes the broadcast storm is displayed.

Repeater Statistics Information

Selecting this option displays the Repeater Statistics Information Menu as shown in Figure 4-29.

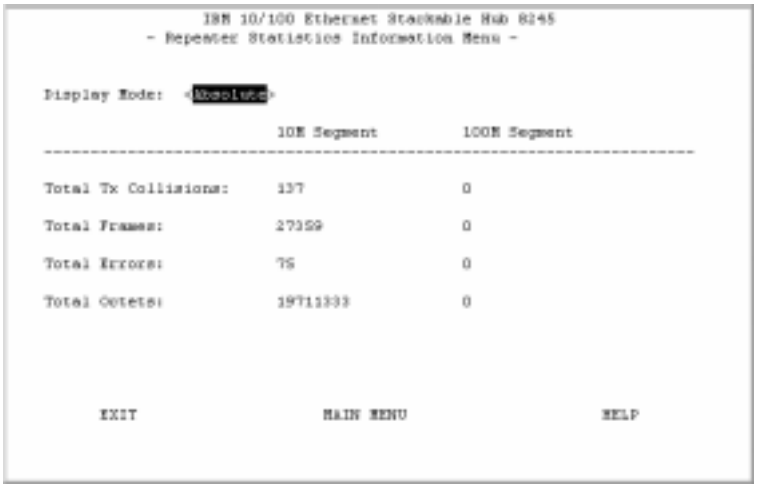


Figure 4-29 Repeater Statistics Information Menu

Display Mode

Displays counters for the 10-Mbps and 100-Mbps segment for all hubs in the stack.

Absolute mode: Select **Absolute** and press **Enter**. Each counter will represent the value collected since system start. You cannot clear absolute counters.

Relative mode: Select **Relative** and press **Enter** key. Each counter will be cleared to 0, and will then redisplay the value collected since the relative mode was selected. You can reset the relative counters to 0 by changing to Absolute Mode and then changing back to Relative Mode.

Total Tx Collisions

The number of transmission collisions that have occurred in this stack.

Total Frames

The number of frames received in this stack.

Total Errors

Total errors received by the stack including FCS errors, align errors, frame too long, short events, late events, very long events and rate mismatches.

Total Octets

The number of octets contained in the valid frames that have been received by this stack.

Repeater Group Statistics Information

Selecting this option displays the Repeater Group Statistics Information Menu as shown in Figure 4-30.

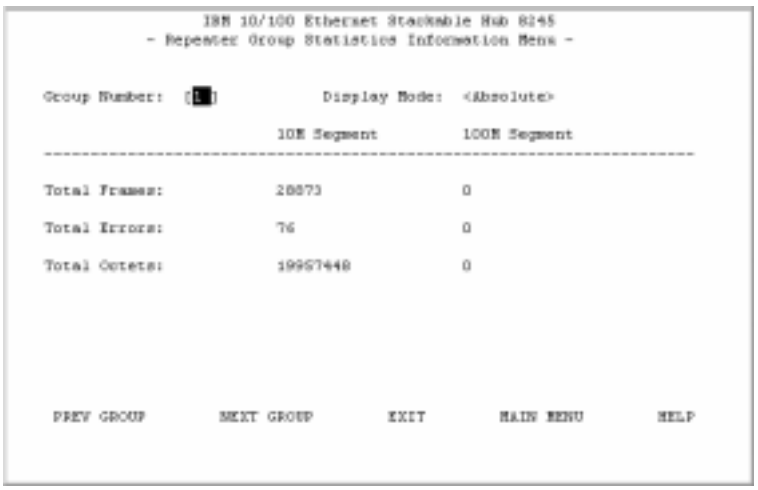


Figure 4-30 Repeater Group Statistics Information Menu (Absolute)

Repeater Group Statistics Information Menu displays statistics information counters for the current port of current hub. Counters are displayed in *Absolute* or *Relative* values by toggling the display mode. Absolute values represent the value collected since system start. You cannot clear absolute counters. Relative counters represent the values collected since the relative mode was selected. You can reset the relative counters to zero by changing to Absolute Mode and then changing back to Relative Mode.

Group Number

The ID number of an 10/100 Ethernet Stackable Hub in the stack (1 to 6).

Display Mode

Display counters in Absolute or Relative values. Relative counters represent the value collected since the relative mode was selected. Absolute values represent the value collected since system start.

Total Frames **0 to 2^{32}-1 (4294967295 decimal)**

The number of frames of valid frame length that have been received on the ports of this hub and not including FCS errors and Collisions.

Total Octets **0 to 2^{32}-1 (10M segment) / 0 to 2^{64}-1 (100M segment)**

The total number of octets contained in the valid frames that have been received on the ports of this hub.

Total Errors **0 to 2^{32}-1**

Total errors received by the port including FCS Errors, Align Errors, Frame Too Long, Short Events, Late Events, Very Long Events, and Rate Mismatch.

Repeater Port Statistics Information

Selecting this option displays the Repeater Port Statistics Information Menu as shown in Figure 4-31.

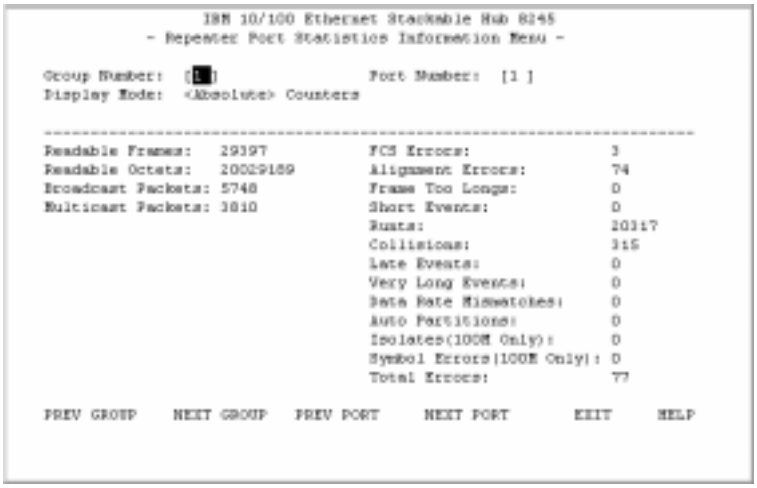


Figure 4-31 Repeater Port Statistics Information Menu

The Repeater Port Statistics Information Menu displays counter information for the current port of the current hub. You can select a hub with the PREV GROUP and NEXT GROUP commands and its ports with the PREV PORT and NEXT PORT commands.

Display Mode

Display counters in Absolute or Relative values. Relative counters represent the values collected since the relative mode was selected. Absolute values represent the value collected since system start.

Group Number

The ID number of an 10/100 Ethernet Stackable Hub in the stack (1 to 6).

Port Number

Port number of selected group (1 to 12/24).

Readable Frames

Total readable frames received by the port.

Readable Octets

Total readable octets received by the port.

Broadcast Packets

The total number of good packets received that were directed to a broadcast address. Note that this does not include multicast packets.

Multicast Packets

The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

FCS Errors

The total number of packets received by the port that had bad Frame Check Sequences.

Alignment Errors

Total Alignment Errors frames within the proper size (64 to 1518 octets) received by the port.

Frame Too Long

Total frames received by the port that were longer than 1518 octets (excluding framing bits, but including FCS octets).

Short Events

Total frames received by the port that were shorter than 64 octets or that had an activity duration shorter than the event, ShortEventMaxTime (74 to 82 bit times).

Runts

The total number of packets received that were less than 64 octets due to collisions or activity duration was greater than the ShortEventMaxTime event and less than the ValidPacketMinTime event.

Collisions

Total collisions.

Late Events

Total number of events received by the port for which the activity duration was greater than the LateEventThreshold.

Very Long Events

Total number of events received by the port for which the activity duration was greater than the MAU Jabber Lockup Protection timer TW3.

Data Rate Mismatches

Total number of frames received by the port with no collisions and for which the activity duration was greater than the ValidPacketMinTime event and the frequency (data rate) was detectable mismatched from the local frames mismatch frequency.

Auto-Partitions

Total number of times the port was auto-partitioned.

Isolates (100M only)

Total isolates for 100-Mbps transmissions. This counter is incremented by one each time that a port automatically isolates as a consequence of false carrier events. The conditions that cause a port to automatically isolate are defined by the transition from the False Carrier state to the Link Unstable state. The port will automatically recover.

Symbol Errors (100M only)

Total symbol errors for 100-Mbps transmissions. This counter is incremented by 1 for each valid length packet received at the port with at least one occurrence of an invalid data symbol. This can increment only once per valid carrier event. The approximate minimum time for rollover of this counter is 7.4 hours at 100 Mbps.

Total Errors

Total errors received by the port including FCS Errors, Align Errors, Frame Too Long, Short Events, Late Events, Very Long Events and Rate Mismatch.

Address Tracking Information

Selecting this option displays the Address Tracking Information Menu as shown in Figure 4-32.

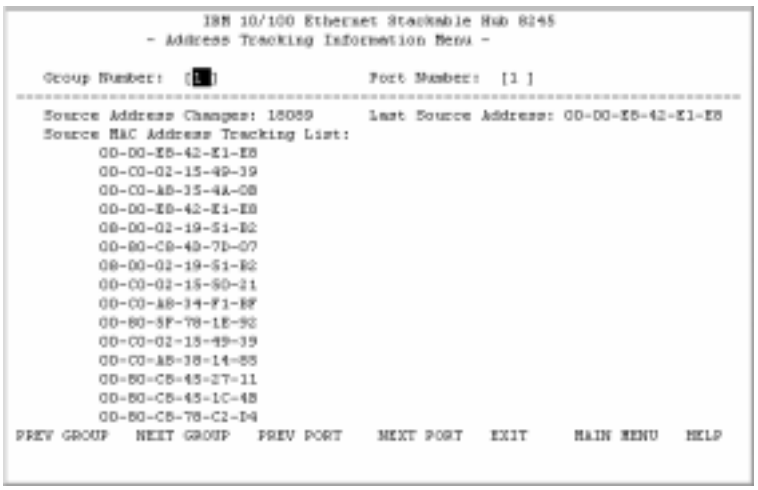


Figure 4-32 Address Tracking Information Menu

The 10/100 Ethernet Stackable Hub 8245 provides per-port based node (MAC address-based) tracking capability. The node tracking function records the source MAC of each data packet and provides the filters for data analysis.

Source Address Changes

This counter is incremented by 1 for each time that the Last Source Address for this port changes. This may indicate whether a link is connected to a single device or another multi-user segment. The approximate minimum time for roll-over of this counter is 81 hours.

Last Source Address

Indicates the source MAC address of the last readable frame received by this port. If this port has received no frames since the hub began monitoring the port activity, a null string will be displayed.

Source MAC Address Tracking List

A list of source MAC addresses that were recently received on this port. The first source MAC address (00-04-AC-1C-80-23) in the tracking list contains the value that is given by the Last Source Address for this port. This list can contain 15 entries. The list does not age out, the first entries are deleted to accommodate new entries when the list is full.

Address Search Information

Selecting this option displays the Address Search Information Menu as shown in Figure 4-33.

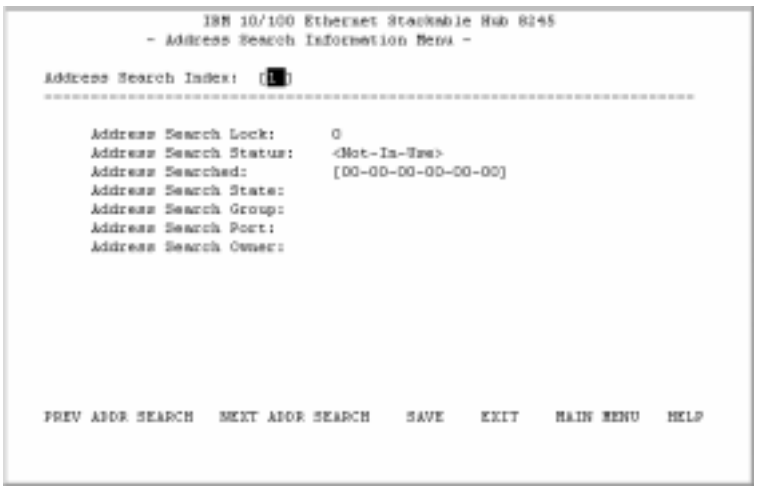


Figure 4-33 Address Search Information Menu

The 10/100 Ethernet Stackable Hub 8245 provides source (MAC address) matching capability on a per-segment basis. The active address tracking capability is used to watch for a given MAC address and report which port it was seen on. This capability can be also used to collect the necessary information for mapping the topology of a network. Up to 8 MAC addresses can be searched simultaneously.

Address Search Index

Identifies the index of the source address to be searched in the system for which this entry contains information (1 to 8).

Address Search Lock

Used by a management station as an advisory lock for a search entry. The search lock increments by 1 if the address is available. The number will be incremented to the maximum value of 2^{32}-1 and then roll over to zero.

Address Search Status

In Use: A management station has obtained ownership.

Not In Use: No other management station has obtained ownership.

A management station first retrieves the values of the appropriate instances of the Address Search Lock and Address Search Status objects, periodically repeating the retrieval if necessary, until the value of Address Search Status is "Not In Use." The management station then tries to set the Address Search Lock *In Use*. If the set operation succeeds, then the management station has obtained ownership of the entry, and the value of Address Search Lock is incremented by 1. Failure of the set operation indicates that some other manager has obtained ownership of the entry.

Address Searched

Specify MAC address for search.

Address Search State

The current state of the MAC address search on this hub.

Single: The hub detects the address on one port only.

Multiple: The hub detects the address on more than one port.

None: The hub does not detect the address of any port.

The state is initially set to none.

Address Search Group

The Hub ID received, whose source address corresponds to the address searched (1 to 6).

Address Search Port

The port number received, whose source address corresponds to the address searched (1 to 24).

Address Search Owner

The entity that currently has *ownership* of this search entry.

The owner for a given address search entry could be one of the following:

CONSOLE: If the entry is locked by the Local Console/Remote Telenet, the owner is CONSOLE.

WEB: If the entry is locked by the Web-based manager, the owner is WEB.

hubrptrAddrSearchOwner: If the entry is locked by the SNMP manager, the owner will be given by the SNMP manager by setting the MIB object hubrptrAddrSearchOwner.

Broadcast Storm Protection

Selecting this option displays the Broadcast Storm Protection Menu as shown in Figure 4-34.

Figure 4-34 Broadcast Storm Protection Menu

The 10/100 Ethernet Stackable Hub 8245 periodically monitors the broadcast counters of each hub port to detect a broadcast storm condition. The hub port that causes the broadcast storm can be automatically partitioned or a trap can be sent to the trap receivers or both. The 10/100 Ethernet Stackable Hub 8245 continually monitors those ports that have been partitioned to check if the broadcast storm condition still exists. The port will be permanently partitioned if the broadcast storm does not subside in 2 minutes.

You can configure the broadcast threshold value for each port, each segment, and each optional module. The Segment Rate Threshold, Port Rate Threshold, and Optional Module Rate Threshold determine whether the broadcast storm exists or not.

Segment ID

The Segment ID specifies the segment where the broadcast storm protection function is applied (10-Mbps/100-Mbps segments).

Segment Broadcast Packet Rate Threshold

The number of broadcast packets received on a given segment per second. The range is 0 to 14,880 packets per second.

Optional Module Broadcast Packet Rate Threshold

The number of broadcast packets received on each uplink of a given optional module per second. The range is 0 to 14,880 packets per second.

Port Broadcast Packet Rate Threshold

The number of broadcast packets received on a given port per second. The range is 0 to 14,880 packets per second.

Broadcast Alarm Action

Once broadcast storm is detected on a given port, segment, or optional module, the proper action is performed based on the value specified by its Broadcast Alarm Action.

Partition Port: The port will be disabled. Once a port is partitioned due to a broadcast storm, the Broadcast Storm protection function will continue to monitor the port. The port is disabled for 15 seconds and re-enabled for 5 seconds. This process is repeated for 2 minutes. If the broadcast storm still exists after 2 minutes, the port is disabled and will no longer be monitored for the broadcast storm.

Note: You must enable the port once the source of the broadcast storm has been handled. You should resolve the broadcast storm before re-enabling the port.

Send-Trap-Partition-Port:
The port will be disabled and a trap will be sent.

Send Trap:
A trap is sent.

No Action:
No action will be taken.

Broadcast Alarm Status

Enable:
Enable the broadcast monitoring and protection function on this segment.

Disable:
Disable the broadcast monitoring and protection function on this segment.

Invalid:
Purge the broadcast monitoring and protection setting for this segment.

Formula for calculating broadcast packet rate

$$\text{Broadcast packet rate} = \frac{\text{Broadcast packet received}}{\text{Seconds}}$$

Configuring broadcast storm protection

To detect the broadcast storm of the 10/100 Ethernet Stackable Hub 8245, configure the following parameters from the Broadcast Storm Protection Menu:

Step 1. Select **100-Mbps Segment** in the **Segment ID** field.

Step 2. Configure **Segment Broadcast Packet Rate Threshold**.

Step 3. Configure **Optional Module Broadcast Packet Rate Threshold**.

Note: The "Optional Module broadcast Packet Rate Threshold" of the 100-Mbps segment is used for both 10-Mbps and 100-Mbps Broadcast Storm Detection.

Step 4. Configure **Broadcast Alarm Action**.

Step 5. Enable the broadcast storm protection function.

To detect the broadcast storm of the AUI module, configure the following parameters from the Broadcast Storm Protection Menu:

Step 1. Select **10-Mbps Segment** in the **Segment ID** field.

Step 2. Configure **Segment Broadcast Packet Rate Threshold**.

Step 3. Configure **Optional Module Broadcast Packet Rate Threshold**.

Note: The Optional Module Broadcast Packet Rate Threshold of the 10-Mbps segment is used for the AUI module broadcast storm detection.

Step 4. Configure **Broadcast Alarm Action**.

Step 5. Enable the broadcast storm protection function.

Broadcast Storm Detected

Selecting this option displays the Broadcast Storm Detected Menu as shown in Figure 4-35.

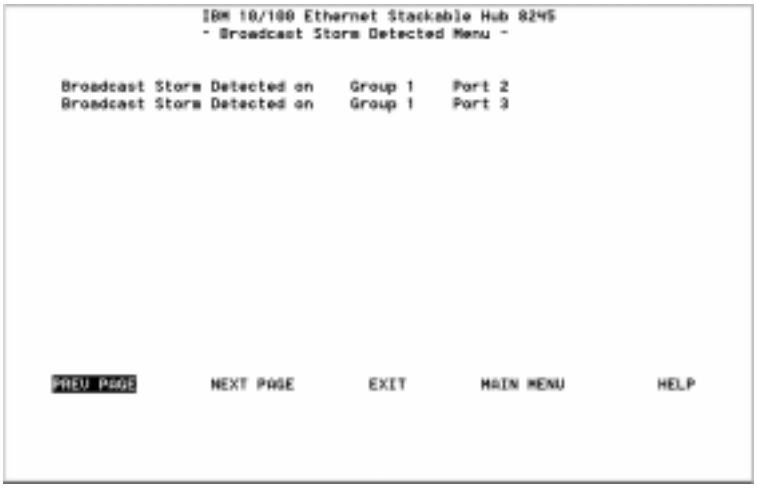


Figure 4-35 Broadcast Storm Detected Menu

For each broadcast storm that is detected, the hub and port number are listed in this menu. If there has been no storm detected, this menu is empty. A maximum of 32 broadcast storms will be displayed, 16 per page. The list is updated on a first-in, first-out basis when the maximum of 32 are reached.

User Authentication

Selecting this option displays the User Authentication Menu as shown in Figure 4-36.

Figure 4-36 User Authentication Menu

This menu lets you define up to six different users. The passwords are the same for both the management session and the Web. You can also change the password for the control panel.

Note: User names and passwords are not case sensitive. To define a user, perform the following steps:

Step 1. Select an index number and press **Enter**.

Step 2. Enter a user name of up to 12 alphanumeric characters.

Step 3. Enter a password of up to 6 alphanumeric characters.

Step 4. Enter the password again to confirm it.

Step 5. Specify **Read Only** or **Read/Write** privilege, and press **Enter**.

Step 6. Select **ADD**.

Step 7. Select **EXIT**.

To change the console password, perform the following steps:

Step 1. Select an index number with a specific user and press **Enter**.

Step 2. Enter a password of up to 6 alphanumeric characters.

Step 3. Enter the password again to confirm it.

Step 4. Specify **Read Only** or **Read/Write** privilege, and press **Enter**.

Step 5. Select **ADD**.

Step 6. Select **EXIT**.

Note: The control panel password can be only four digits (0 to 9). The default is "0000".

The 10/100 Ethernet Stackable Hub 8245 comes with two default user names:

Admin requires no password.
Guest has a password of "guest."

Note: If you do not confirm the password or if the password is incorrect in the confirm field, then it will display the message, Invalid Password. Press **Esc** to continue.

System Utility

Selecting this option displays the System Utility Menu as shown in Figure 4-37.

Figure 4-37 System Utility Menu

The System Utility Menu lets you download microcode, restart the hub, reset the hub to the factory default, set the login timeouts, configure the upload settings, and request an upload.

System Download

Configure type of download.

System Restart

Restart the hub.

Factory Reset

Reset to factory configuration.

Login Timeout Interval

Set the time duration before Telnet or local console automatically logs out.

Configuration Upload Setting

Set the IP Address of the server and the file name to be uploaded.

Configuration Upload Request/Status

Submit a request for a configuration file upload.

System Download

Selecting this option displays the System Download Menu as shown in Figure 4-38.

Figure 4-38 System Download Menu

This menu lets you perform a BootP request and a TFTP code download. To request an IP address, subnet mask, and a default gateway address from your BootP server, perform the following steps:

Step 1. Select **BootP REQUEST**.

Note: Not all DHCP servers support basic BootP services. If you experience a problem, check your DHCP server manual.

Step 2. Perform a cold restart on your system. For information on restarting your system, see “System Restart” on page 4-63.

You should perform a code download only to update existing software or if existing code has become corrupted. Before performing a system download, make sure that you know the IP address of your TFTP server and the location of the files on the server.

Notes: Use the following naming conventions:

1. Boot ROM Code Download - 8245Vxxx.BT
2. Web Pages Database Information Download - 8245Vxxx.WEB
3. System Software Download - 8245Vxxx.RT

where xxx is the version number.

To download TFTP code, perform the following steps:

Step 1. Enter the IP address of the TFTP server.

Step 2. Select the downloads that you want to perform.

Step 3. Enter the path and file name for each of the downloads you have selected (for example, C:\microcode\8245V110.BT).

Step 4. Save the configuration.

Step 5. Restart the system using a cold start.

The backup managed unit will automatically run a system download with the updated setup from the active managed unit whenever it detects a system download has occurred on the active managed unit.

System Restart

Selecting this option displays the System Restart Menu as shown in Figure 4-39.

Figure 4-39 System Restart

The System Restart Menu lets you perform a *cold* or *warm* restart.

You can restart the system at any time without losing configuration settings, except in the case of a download. When you select **EXECUTE** and then press **Enter**, a warning message informs you that system restart will be performed.

Warm

A warm restart restarts the hub at the runtime code. For most cases, a warm restart is sufficient, except in the case of a BootP request or code download.

Cold

A cold restart restarts the hub at the Boot ROM level and is the same as unplugging and replugging power to the hub. A cold restart is needed when the user performs a BootP request or code download.

Factory Reset

Selecting this option displays the Factory Reset Menu as shown in Figure 4-40.

Figure 4-40 Factory Reset Menu

The Factory Reset Menu lets you return all hub settings to the original default settings.

When you issue a factory reset, all of your custom settings are overwritten.

To perform the factory reset, perform the following steps:

Step 1. Select how you want the network configuration to be processed during a factory reset:
- **Not Reset –** Current network configuration is saved.
- **Reset from BootP –** Request a new network configuration from BootP server.
- **Reset to factory default –** Current network configuration is reset to factory defaults.

Step 2. Select how the user authentication configuration will be processed during a factory reset:
- **Not Reset –** Current user authentication configuration is saved.
- **Reset to factory default –** Current user authentication configuration returns to factory defaults.

Step 3. Select **EXECUTE** and press **Enter**.

A warning message informs you that system configuration data will be reset now.

Login Timeout Interval

Selecting this option displays the Login Timeout Interval Menu as shown in Figure 4-41.

Figure 4-41 Login Timeout Interval Menu

This menu lets you select the time after which an established Telnet session or Local Console is automatically logged out if inactive. The range is 0 to 60 minutes. The default is 5 minutes. If you specify 0, the session remains logged in regardless of how long it is inactive.

Select **SAVE** to save your changes.

Configuration Upload Setting

Selecting this option displays the Configuration Upload Setting Menu as shown in Figure 4-42.

Figure 4-42 Configuration Upload Setting Menu

The 10/100 Ethernet Stackable Hub 8245 can upload the hub configuration data to the remote server in binary format. You can upload your configuration files and save them as a backup in case you need to restore your system settings.

Enter the TFTP Server IP Address and the chosen file name (for example: *filename*.CFG) and the path where the files will be uploaded to the server. Select **SAVE** to save your configuration settings, and then request the upload using the Configuration Upload Request Menu. See “Configuration Upload Request” on page 4-67.

TFTP Server IP Address

The IP address of the server on which the configuration files are to be stored.

Configuration File Name

The name of the configuration file and the full path of the location where the files will be saved on the server.

Configuration Upload Request

Selecting this option displays the Configuration File Upload Request/Status Menu as shown in Figure 4-43.

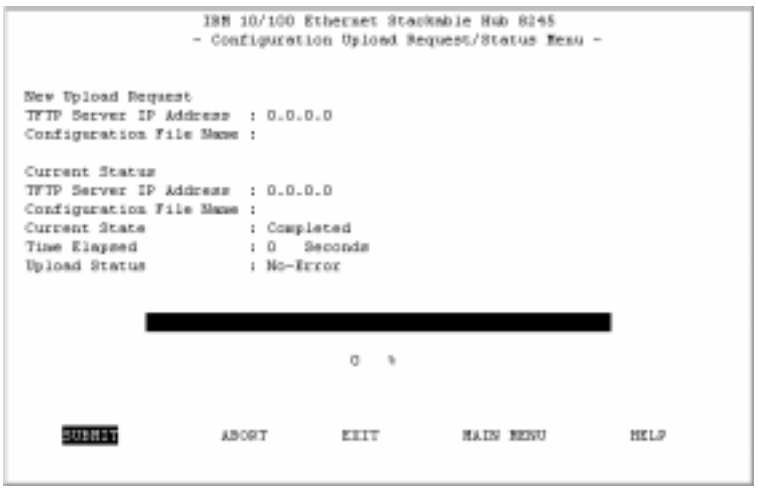


Figure 4-43 Configuration File Upload Request/Status Menu

This menu displays information only. See Figure 4-43 as an example. To edit configuration upload settings, see “Configuration Upload Setting” on page 4-66.

Select **SUBMIT** to make the upload request.

TFTP Server IP Address

The IP address of the server that the configuration files will be uploaded to.

Configuration Filename

The name of the configuration file and the full path.

Current State

When the configuration file download is complete, **COMPLETED** is displayed.

Time Elapsed

The time elapsed since starting the upload request.

Upload Status

The status of the data transfer with regard to errors.

No Error

The upload was successfully stored in the specified configuration file.

No-Such-File

The path specified in the Configuration Filename field, cannot be found on the TFTP Server.

Access Violation

The file specified in the Configuration Filename field is Write Protected.

Disk Full

The disk specified in the Configuration Filename field, is full.

Timeout

The TFTP upload timeout of 20 seconds has expired. A progress bar is displayed in the menu showing the progress.

Other Error

Other errors that are defined by the system.

Once you have uploaded your configuration files you can download them if necessary. See “System Download” on page 4-61 for information about downloading configuration files.

Chapter 5. Using Web Management

You can use your Web browser to configure the 10/100 Ethernet Stackable Hub. Enter the hub’s IP address or host name in your Web browser's address field. You are prompted for a user name and password.

The 10/100 Ethernet Stackable Hub comes with two default user names. One default is “admin” and requires no password. The other default is “guest” and has a password of “guest.” (User names and passwords are not case sensitive).

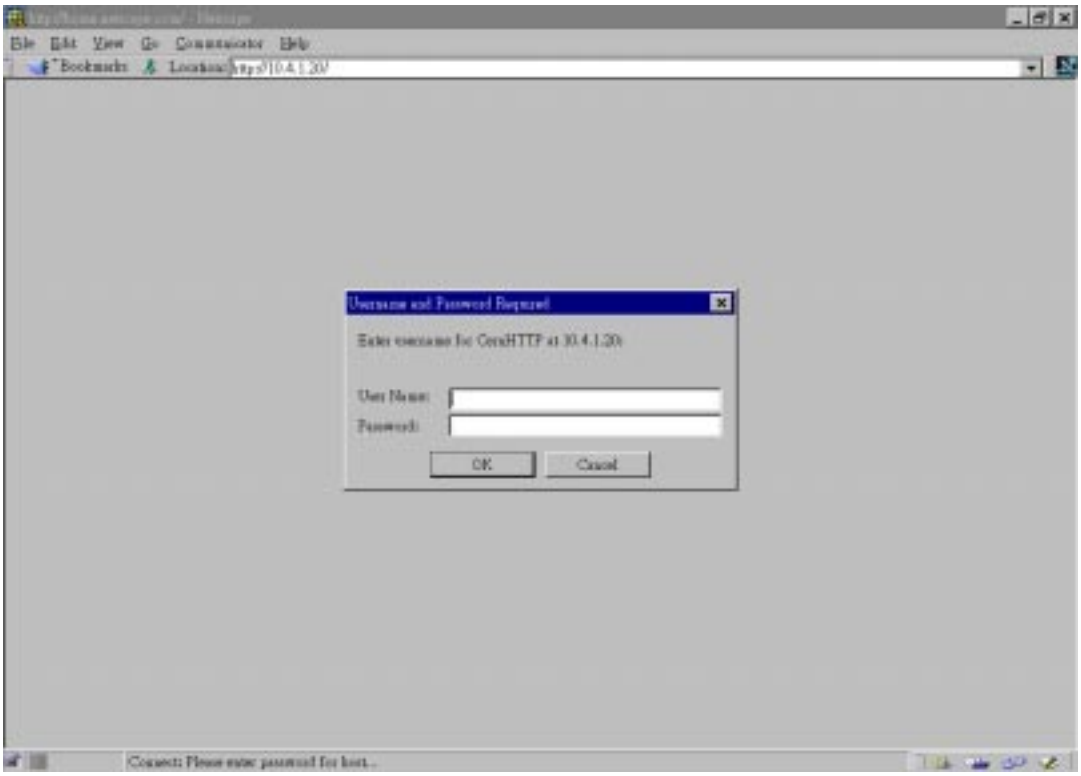


Figure 5-1 Login Menu

Home Page

After you log in, the 10/100 IBM Ethernet Stackable Hub 8245 home page is displayed as shown in Figure 5-2. This menu also contains a link to the IBM home page (*www.ibm.com*).

Figure 5-2 Home page

The Home Page displays the following menus:

System Information

Provides information related to the version of the system software installed on the hub.

Management Setup

Allows you to set up the management functions of the hub.

Device Control

Allows you to configure the hubs and their ports.

Network Monitor

Allows you to configure network monitoring.

RMON

Allows you to configure remote monitoring.

System Utility

Allows you to use and configure the system utilities.

Help

Displays help guide for Microsoft Internet Explorer users and shows how to enable the trap window.

Trap Frame Window

The Trap Frame window is displayed when the Web browser connects to the 10/100 Ethernet Stackable Hub 8245 as shown in Figure 5-3.

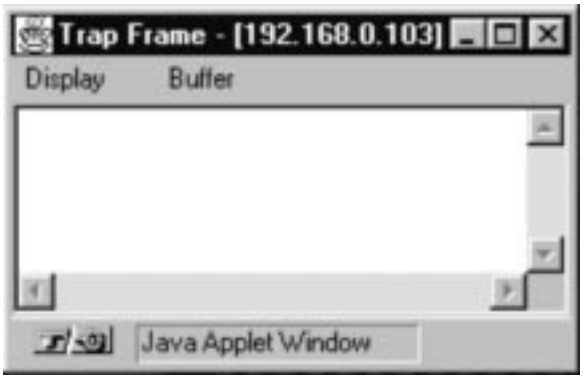


Figure 5-3 Trap Frame Window

This window receives all traps from the hub except for cold start, Hello, and RMON traps. The maximum number of traps displayed depends on system resources and capacity.

Display

Lets you manage how you want to display traps:

Pause: Stops displaying any new traps.

Continue: Resumes displaying new traps.

Clear: Clears the traps displayed on the Trap Frame window.

Buffer

Lets you control the traps in the buffer:

Delete: Deletes all the traps in the buffer.

Dump: Dumps all the traps in the buffer to the Trap Frame window.

Hub Graphic

The graphic picture of the 10/100 Ethernet Stackable Hub 8245 displayed in the top section of each of the Web pages is a Java applet that allows you to view the hub.

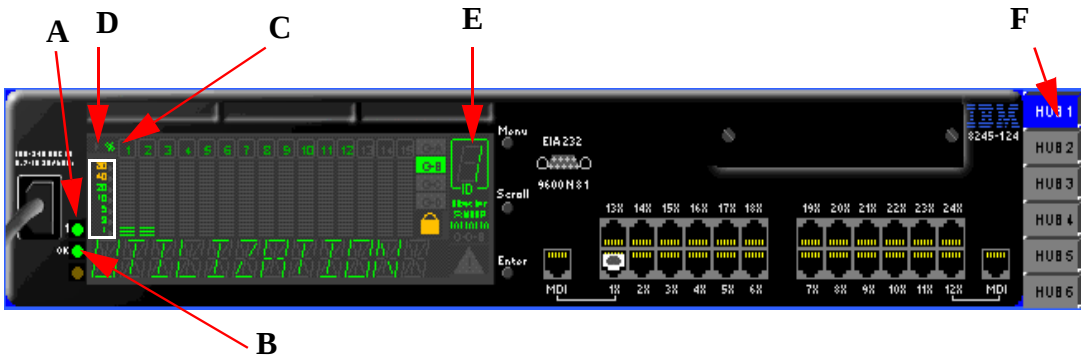


Figure 5-4 Hub Graphic of the Managed Unit

Managed Hub Graphic

The Managed Hub Graphic displays a graphical picture of the 10/100 Ethernet Stackable Hub.

Hub Icon

Selecting the hub icon displays a graphical picture of the hub and shows its current status. (see F)

- **Green:** A manageable hub or a manged hub that is not active.
- **Blue:** An active managed hub.
- **Gray:** A hub is disconnected or is unavailable.

Hub ID

A range of 1 to 6 indicates that the Hub ID of the connected hub (see E).

The following indicators are always on (as shown in Figure 5-4):

- | (LED): AC power status. (see A).
- OK (LED): (see B).
- %: (see C).
- Ticker Scale (1, 3, 5, 10, 20, 40, 80): (see D).
- Lock Sign

Port Indicators

Indicates a port number.

Gauge Bars

Displays port-related information such as utilization.

Message Zone

Automatically switches between the “Utilization” and “10M 100M.”

G-A

Displays status of ports 1 to 12 in Port Group A.

G-B

Displays status of ports 13 to 24 in Port Group B.

Master

Indicates that the hub is a managed hub.

SNMP

Indicates that the hub is SNMP-manageable.

OOB

Indicates that the out-of-band is enabled.

Menu Key

Not used.

EIA 232 Connector

By clicking on it with the right mouse button, a pop-up menu appears allowing you to display console information, OOB SLIP setup, and OOB baud rate.

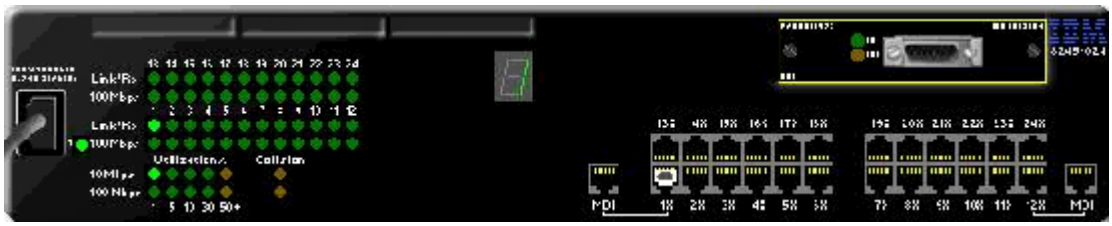


Figure 5-5 Hub Graphic of the Manageable Unit

Manageable Hub Graphic

Selecting the hub icon displays a graphical picture of the manageable hub showing its current status.

LED Status

- **| (LED):**

  -Always On

- **Link/Rx LEDs:**

  -Off: Link down

  -Green: Link up

  -Green and blinking: Packet receiving

- **100-Mbps LEDs:**

  -Off: 10-Mbps speed

  -Green: 100-Mbps speed

- **Collision LEDs:**

  -Amber: Collision detected

  -Off: No collision

- **Utilization Indicators:**

  - Five LED levels show the utilization of 10-Mbps and 100-Mbps segments.

  Note: Five 10-Mbps segment utilization LEDs (green, green, green, green, amber). Five 100-Mbps segment utilization LEDs (green, green, green, green, amber).

- **TP Port Connector**

  -White (inside inner frame): Link up

  -Amber (inner frame): auto-partitioned

  -White (frame): admin disabled

Optional Modules

There are three optional modules that can be installed in the 10/100 Ethernet Stackable Hub. The modules are the 10BASE-T/100BASE-TX bridge module, the 100BASE-FX bridge module, and the AUI expansion module.

10BASE-T/100BASE-TX Module

Figure 5-6 10BASE-T/100BASE-TX Module

The following indicators are always off on the Java applet of the hub graphical display:

- TX
- RX
- COL

The following indicators are either on or off:

- Link
- FDX
- 100-Mbps
- Int Bridge Ena

How to Map the Hub's Admin State to the Legend of the Graphic

- **Internal Hardware Admin State**
  This depends on the Int Bridge Ena LED and the border color of the module.
  LED on: Enabled
  LED off: Disabled
  Border Color
  None: Enabled
  Yellow: Disabled
- **Internal Function Admin State**
  This depends on the border color of the module.
  Border Color
  None: Enabled
  Yellow: Disabled
- **External Function Admin State**
  The appearance of the uplink module port will change depending on the status of the port and the appearance is the same as the TP port.

100BASE-FX Module

Figure 5-7 100BASE-FX Module

The following indicators are always off on the Java applet of the hub graphical display:

- TX
- RX
- COL

The following indicators are either on or off:

- Link
- FDX
- Int Bridge Ena

How to Map the Hub's Admin State to the Legend of the Graphic

- **Internal Hardware Admin State**
  This depends on the Int Bridge Ena LED and the border color of the module.
  LED on: Enabled
  LED off: Disabled
  Border Color
  None: Enabled
  Yellow: Disabled
- **Internal Function Admin State**
  This depends on the border color of the module.
  Border Color
  None: Enabled
  Yellow: Disabled
- **External Function Admin State**
  Link Down
  Black Inside: Enable
  White Inside: Disable
  Link Up
  Gray: Enable

White: Disable

AUI Expansion Module

Figure 5-8 AUI Expansion Module

The following indicators are always off on the Java applet of the hub graphical display:

- RX
- COL

How to Map the Hub's Admin State to the Legend of the Graphic

- **External Software Admin State**

  Black Inside: Enable

  White Inside: Disable

Port Selections for the Hub

If you click the right mouse button on any port, a menu is presented. You can use the left mouse button to make the following port selections:

Statistics

Displays the Repeater Port Statistics Information Menu for the selected port.

Control

Lets you enable or disable ports:

ADMIN Enable: Enables the selected port.

ADMIN Disable: Disables the selected port.

The port status of the individual ports are graphically displayed in Figure 5-9.

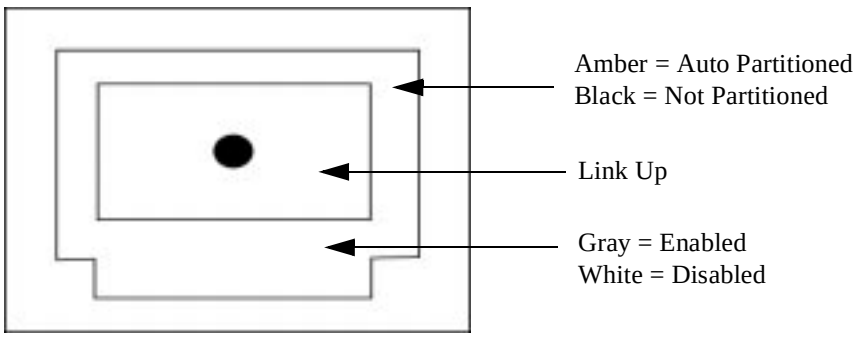


Figure 5-9 Hub Port Status Legend

Unit Selection

If you click the right mouse button on the unit itself, a menu is presented. You can use the left mouse button to make the following unit selections:

INFO

Displays the Repeater Group Control/Status Menu for the unit.

STATISTICS

Displays the Repeater Statistics Information Menu.

TRAP

Opens a trap window for the specified hub if its trap window was not already displayed.

System Information

Selecting this option displays the System Information Menu as shown in Figure 5-10.

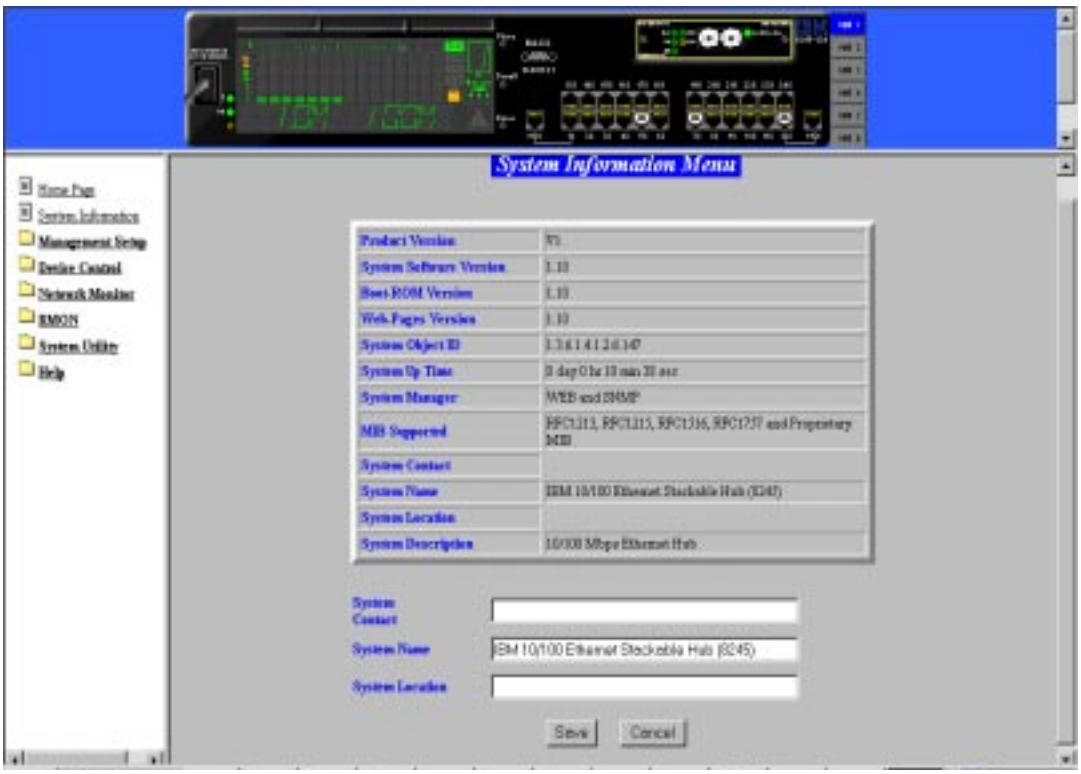


Figure 5-10 System Information

The System Information Menu provides information related to the version of the system software installed on the 10/100 Ethernet Stackable Hub 8245.

You can specify up to 48 alphanumeric characters for each of these: System Contact, System Name, and System Location to provide useful information to all users concerning the hub. The information on this menu should be kept current so that persons requiring assistance know whom to contact.

Notes:

1. Select **SAVE** before you exit this menu to save any changes you have made.
2. The MIBs supported field is for information only.

System Description

A textual description of the entity. This also includes the name and version identification of the system's hardware type, software operating system, and networking software.

System Object ID

The vendor's authoritative identification of the network management subsystem is contained in the 10/100 Ethernet Stackable Hub. This value is allocated within the SMI enterprises' subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of device is being managed.

System Manager

The management capability that this system supports (SNMP and WEB).

System Up Time

The time since the network management portion of the system was last restarted or powered on.

Management Setup

Selecting this option displays the following options:

Network Configuration

Sets the IP address, Subnet Mask, and Default Gateway address.

Serial Port Configuration

Configures the serial port for communications.

SNMP Community

Configures community names and access.

Trap Receiver

Sets up community trap addresses.

Trap Filter

Sets up trap filters.

IPX Address Configuration

Sets the device's IPX address.

IPX Trap Receiver

Sets the locations to receive the SNMP traps for IPX.

Network Configuration

Selecting the Network Configuration Menu allows you to select the Network Configuration-Ethernet Menu as shown in Figure 5-11 and the Network Configuration-SLIP Menu as shown in Figure 5-12 on page 5-17.

Note: The 10/100 Ethernet Stackable Hub 8245 must be restarted for the changes to take effect. For information on restarting the HUB, see “System Restart” on page 5-87.

Ethernet Menu

An Ethernet connection allows you to monitor and configure the hub with a local console via Telnet session, a Web browser, or SNMP management. You need to configure the ID address, and Subnet Mask to work with your LAN settings before you can make an Ethernet connection.

Figure 5-11 Network Configuration-Ethernet Menu

Current Configuration

The IP configuration that is currently running on the hub.

IP Address

The dotted decimal IP Address assigned to the hub.

Subnet Mask

The dotted decimal Subnet Mask assigned to the hub.

Default Gateway

The dotted decimal IP address of the default router assigned to the hub.

New Configuration

The IP configuration that will become the new current configuration when the hub is restarted.

The 10/100 Ethernet Stackable Hub 8245 must be restarted before the IP address, subnet mask, and default gateway can take effect. To ensure that the new information is correct, do a “ping” from another device that is connected to the hub.

Note: The hub does not respond to ping packets that are greater than 1484 bytes.

SLIP Menu

SLIP connections enable monitoring and configuring of the 10/100 Ethernet Stackable Hub.

Figure 5-12 Network Configuration-SLIP Menu

The baud rate, character size, parity, and stop bits are read only and not configurable on this menu.

Baud Rate

The current serial port baud rate that can be configured from the Serial Port Configuration Menu.

Character Size

8 bits.

Parity

None.

Stop Bits

1 stop bit.

Current Configuration

The SLIP configuration that is currently running on the hub.

New Configuration

The SLIP configuration that will become the new current configuration when the hub is restarted.

IP Address

The dotted decimal address assigned to the SLIP interface of the hub.

Subnet Mask

The dotted decimal subnet mask assigned to the hub.

Serial Port Configuration

The Serial Port Configuration Menu allows you to view Console and configure SLIP connections.

Console

Selecting this option displays the Serial Port Configuration-Console Menu as shown in Figure 5-13. The console is used to view the configurations required to make a VT100 terminal emulator connection to the 10/100 Ethernet Stackable Hub.

Figure 5-13 Serial Port Configuration-Console Menu

Note: The information displayed on this menu is read only and these are the settings required when making a console connection to the 10/100 Ethernet Stackable Hub 8245.

Out-Of-Band

Selecting this option presents the Serial Port Configuration-Out-Of-Band menu as shown in Figure 5-14. Out-Of-Band mode enables you to set serial port configurations for making a connection to the 10/100 Ethernet Stackable Hub 8245 management port using a modem.

Figure 5-14 Serial Port Configuration-Out Of Band Menu

Current Configuration

The current out-of-band (OOB) configuration.

New Configuration

The new OOB configuration that will be updated after you select **SAVE**. You must restart the hub before settings take effect.

Baud Rate

You can set the baud rate to any of the following: 2400, 4800, 9600, or 19200 bps. The default is 9600.

Character Size

8 bits.

Parity

No parity.

Stop Bits

1 stop bit.

When SLIP is enabled, the EIA 232 port can be used for SLIP only. The EIA 232 port cannot be used to gain access to a management session via VT100 terminal emulation.

EIA 232 Port

When you place your cursor on the EIA 232 port of the device and click on the right mouse button, a selection between **CONSOLE INFO**, **OOB SLIP, OOB Baud Rate** for Serial Port Configuration appears for you to choose.

You can click on **CONSOLE INFO** and see the current information being displayed on the Serial Port Configuration-Console Menu, click on the **OOB SLIP**, which allows you to set the IP address and/or subnet mask, or click on the **OOB Baud Rate**, which allows you to change the baud rate of OOB SLIP.

SNMP Community Setup

Selecting this option displays the SNMP Community Setup Menu as shown in Figure 5-15.

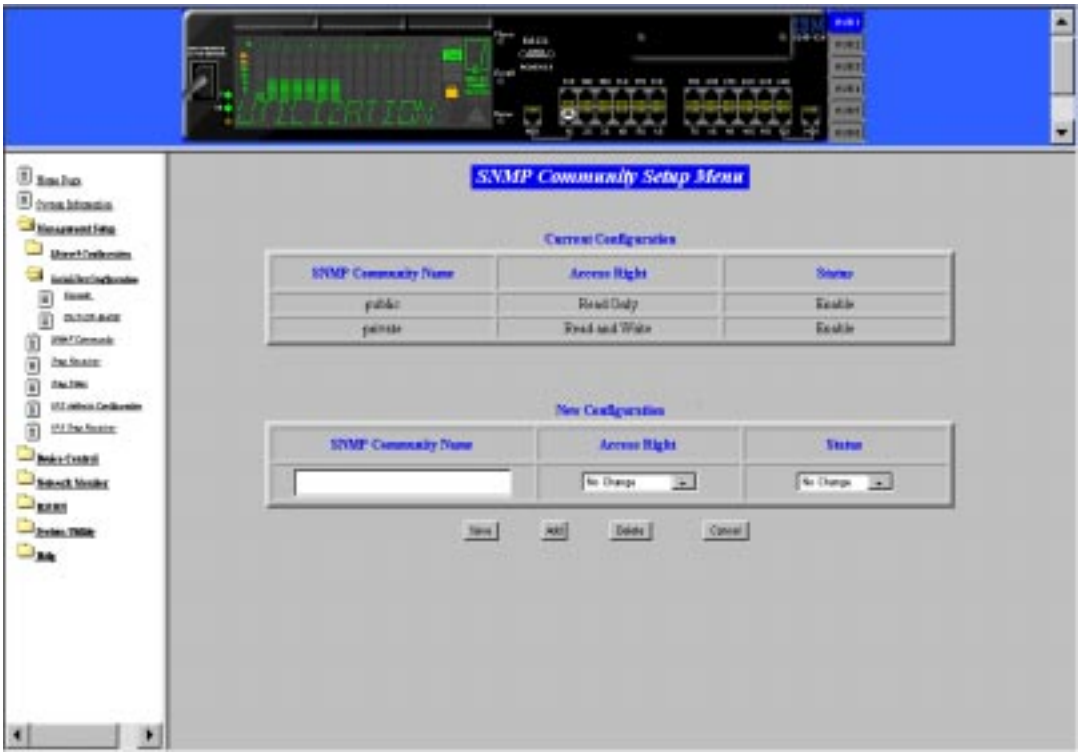


Figure 5-15 SNMP Community Setup Menu

The SNMP Community Setup Menu enables you to configure up to six community names. You can add or edit SNMP community names and set the access right and status. Community names are *case sensitive*. For example, “Private” and “private” are considered different.

SNMP Community Name

A valid community name that exists in the SNMP Community. The names “public” and “private” are already entered, allowing you to use the SNMP community without any configuration settings. These two community names can be edited or renamed as well as any new community names added. It consists of a text string up to 16 characters.

Access Right

You can configure the Access Right to **Read Only** or **Read and Write**.

Status

The status of community names (Enable or Disable):

Enable: To enable an SNMP community.

Disable: To disable an SNMP community.

To add a community name:

Step 1. Select **Management Setup** from the Main Menu.

Step 2. Select **SNMP Community Setup**. The SNMP Community Setup Menu is loaded.

Step 3. Enter a Community name. Entering an existing name will overwrite the existing name when saved.

Step 4. Set the **Access Right**.

Step 5. Set the **Status**.

Step 6. Select **Add** to add the new community name. Select **SAVE** to update.

Step 7. Repeat steps 3 through 6 for each additional name.

Trap Receiver Setup

Selecting this option displays the Trap Receiver Setup Menu as shown in Figure 5-16.

Figure 5-16 Trap Receiver Setup Menu

Traps are sent across a network to an SNMP Network Manager. These messages alert the manager to changes in the 10/100 Ethernet Stackable Hub 8245. You can define up to six trap receivers to receive traps when network events occur.

Index Number

A number to identify a trap receiver (1 to 6).

Community Name

The SNMP community string of the remote network manager (maximum of 16 characters).

IP Address

The IP address of the remote network manager station to which traps should be sent.

Status

Active or inactive. When set to **Active** the trap receiver will receive traps when a trap event is raised.

To set up trap receivers:

Step 1. Enter an Index number, Community Name, IP Address, and Status.

Step 2. Select **SAVE**.

Step 3. Repeat steps 1 and 2 for each new trap receiver.

Trap Filter

Selecting this option displays the Trap Filter Menu as shown in Figure 5-17.

Figure 5-17 Trap Filter Menu

This menu lets you enable or disable trap filters for those traps defined by RFC1215 and RFC1516. Enabled trap filters send traps to the trap receivers when the associated events occur. The default is all traps enabled.

IPX Address Configuration

Selecting this option displays the IPX Address Configuration Menu as shown in Figure 5-18.

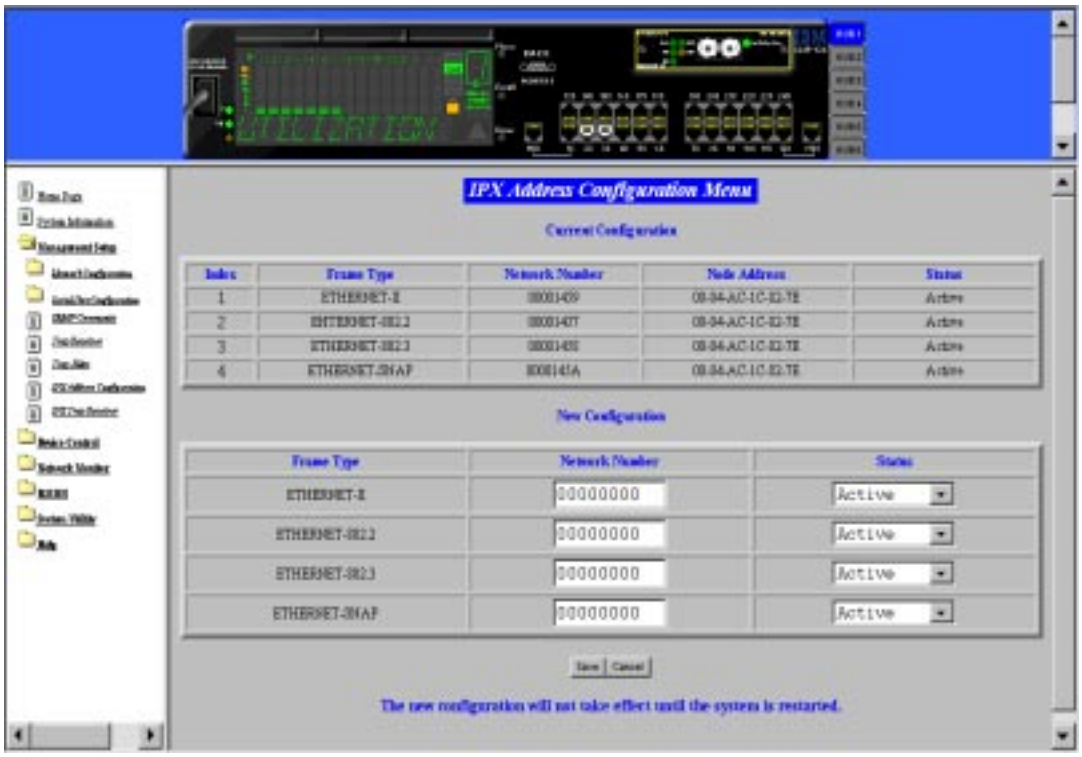


Figure 5-18 IPX Address Configuration Menu

The IPX Address Configuration Menu allows you to set or configure the IPX address of this system.

The menu provides two regions: Current Configuration and New Configuration. The Current Configuration (read only) refers to the configuration that is currently applied in the IPX module. The New Configuration (read/write) refers to the new settings applied, which take effect when the system is restarted.

Frame Type

Each frame type corresponds to one network interface. Select the data link protocol used from among these four available protocols:

- Ethernet-II
- Ethernet-802.2
- Ethernet-802.3
- Ethernet-SNAP

Network Number

There is a network number for each frame type. When the system is restarted, it learns this automatically from the IPX router. If there is no IPX router to supply this information, the default setting will be applied. If the default setting is zero, the agent will self-configure with a unique number as its network number.

Node Address

This field is always the same as the device's MAC address.

Status

You can make certain frame types active or inactive to control the devices. Making a frame active will allow its associate frame type to access it. Making a frame inactive will close the associate frame type.

Select **SAVE** to retain the new configuration. The hub must be restarted before the new configuration takes effect.

IPX Trap Receiver

Selecting this option displays the IPX Trap Receiver Menu as shown in Figure 5-19.

Figure 5-19 IPX Trap Receiver Menu

The IPX Trap Receiver Menu allows you to configure the Trap Receiver through the IPX network. You can set up to six IPX Trap Receivers.

Index Number

A number to identify a trap receiver (1 to 6).

Community Name

The authorized SNMP community string of the remote network manager (maximum of 16 characters).

IPX Address

The IPX address of the remote network manager station to which traps should be sent.

Status

Active or Inactive. When set to Active the trap receiver will receive traps when a trap event is selected.

To set up trap receivers:

Step 1. Enter an Index Number, Community Name, IPX Address, and Status.

Step 2. Select **SAVE** when editing an existing entry.

Step 3. Repeat steps 1 and 2 for each new trap receiver.

Device Control

The Device Control Menu displays the following menus:

Repeater Group Control/Status
Configure the hubs.

Repeater Port Control/Status
Configure the ports.

Bridge Module Control/Status
Configure the bridge module.

External AUI Module Control/Status
Configure the external AUI module.

Redundant Links Control
Configure redundant links.

Security Intrusion Control/Status
Configure security intrusion.

Repeater Group Control/Status

Selecting this option displays the Repeater Group Control/Status Menu as shown in Figure 5-20.

Figure 5-20 Repeater Group Control/Status Menu

You can view the status and configure each hub in the 10/100 Ethernet Stackable Hub 8245 stack or reset to the default setting.

To configure a hub in the stack:

Step 1. Select a 10/100 Ethernet Stackable Hub Group number (Hub ID).

Step 2. Select **Submit** to load the hub's configuration settings.

Step 3. Edit the current configurations.

Step 4. Select **Save** to update the new configuration.

Port Capacity

The number of ports that the selected hub has available (12 or 24).

Repeater Type

The type of hub that is selected. For example, 10/100-Mbps Class-II.

Group Role

The role of the selected hub (managed or manageable).

HW Revision

The hub base board hardware version.

Group Software ID

The software ID number of the hub.

Group Last Change

The following events will cause a group last change:

- A hub connected to or removed from the stack
- A hub restarted
- A device or module is added to the system
- A change in the value of hub operational status
- Ports were added or removed as members of the hub (such as group admin enabled or disabled)
- Any of the counters associated with this hub reset

Group Partitioned Ports

The total number of ports in the hub group that have been auto-partitioned by the hub due to broadcast storm or excessive collisions.

Group Operation

The current status of this group:

Operational: The hub is connected to the stack.

Not present: The hub is not present in the stack.

Group Admin State

Enable or disable the specific group segment. The default value is Enabled All.

No Change: None of these will be modified.

Enabled 10: Only the 10-Mbps segment of a given group is connected to the backplane of the stack. The 100-Mbps segment of a given group is isolated from the stack.

Enabled 100: Only the 100-Mbps segment of a given group is connected to the backplane of the stack. The 10-Mbps segment of a given group is isolated from the stack.

Enabled All: Both 10-Mbps and 100-Mbps segments of a given group are connected to the backplane of the stack. This is the default.

Disabled All: Both 10-Mbps and 100-Mbps segments of a given group are isolated from the stack.

Group Reset

All, some, or none of the group's functions can be changed by selecting one of these options:

No Change: No modifications are made.

Reset All: The function logic, counters, and hub configuration of group will be reset. This is identical to hardware reset (cold start).

Function Only: The function logic of group will be reset. The counters and hub configuration will be held static and will not be reset. This reset operation will reset the link status of each port to 'Link Down' that can cause a Link Status Change event to be raised.

Counters Only: The counters of each port will be reset to 0 but the function logic and hub configuration will be held static and will not be reset.

Note: The selected option takes effect after **SAVE** is selected.

Group Name

The name assigned to this hub, up to 28 characters (cannot be accessed by SNMP Manager).

Group Last Change Notify

Enabled: Send out a trap when the value of 'Group Last Change' is changed.

Disabled: The default. A trap is not sent out when the Group Last Change Notify is changed.

Repeater Port Control/Status

Selecting this option displays the Repeater Port Control/Status Menu as shown in Figure 5-21 and Figure 5-22 on page 5-36.

Figure 5-21 Repeater Port Control/Status Menu (Top/Upper View)

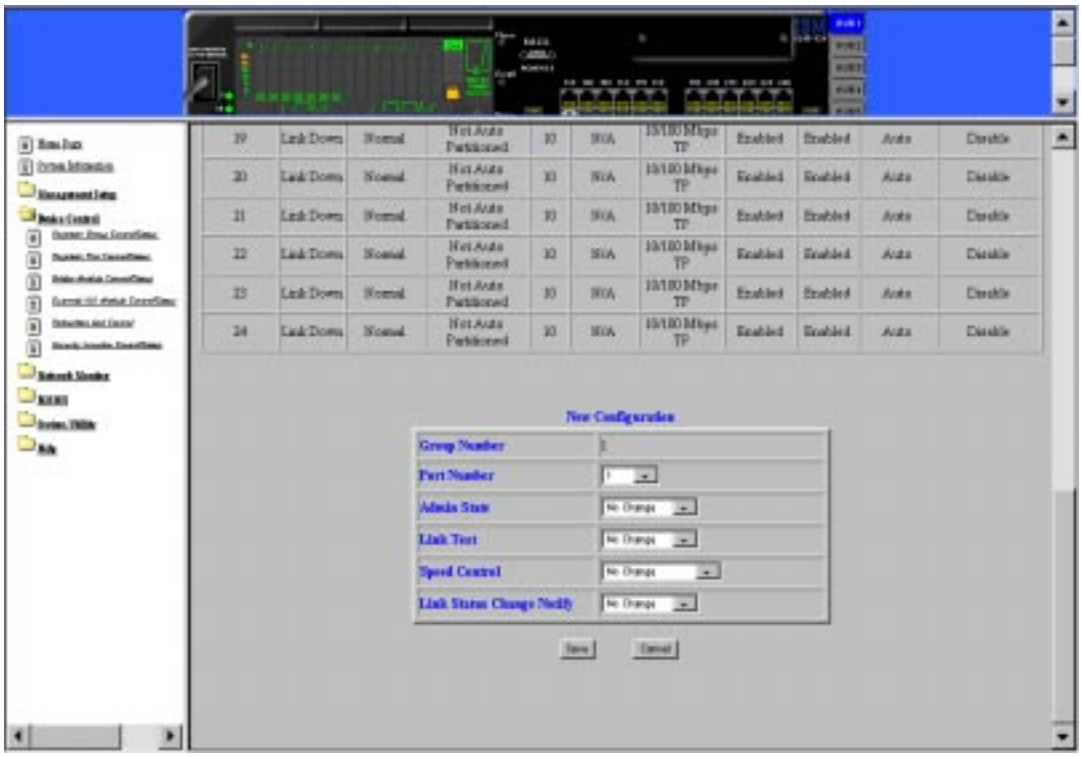


Figure 5-22 Repeater Port Control/Status Menu (Bottom/Lower View)

You can select a group (hub) from the group number pull-down menu and then select **Submit**.

To configure a port on a 10/100 Ethernet Stackable Hub in the stack:

Step 1. Select a port from the Port Number pull-down menu (1 to12 or 1 to 24).

Step 2. Select **Submit** to load the port's current configuration settings.

Step 3. Configure the port.

Step 4. Select **SAVE** to update the new port configuration.

Step 5. Repeat steps 1 through 4 for each port.

Group Number

A 10/100 Ethernet Stackable Hub ID in the stack (1 to 6).

Port Number

The current port number of the current hub.

Link Status

The current link status of the port:

Link Down: Link pulses are not detected on this port.

Link Up: Link pulses are being received on this port.

Polarity Status

The current polarity link status of the port:

Rx Polarity Normal: The receive polarity of the given port is not reversed.

Rx Polarity Reversed: The receive polarity of the given port is reversed and has been automatically crossed by the hub.

Auto-Partition

The current partition status of the port:

Not Auto-Partitioned: The port is not partitioned.

Auto-Partitioned: The port is partitioned.

Speed

The current speed of the port (10 Mbps/100 Mbps).

Isolate Status (100-Mbps port only)

Indicates whether this 100-Mbps port is currently isolated by the repeater

Not Isolated: The port is not isolated.

Isolated: The port is isolated.

Interface Type

The interface type of the port (10/100-Mbps TP port interface type).

Admin State

The current administration state of the port (enabled/disabled).

Link Test

Enable or disable link testing.

Notes:

1. When port link test function is disabled, the Port Link Status always returns Link Up for 10-Mbps ports.
2. Redundant link pairs must have link test enabled.

Speed Control

The port speed. The port will automatically connect to the 10-Mbps or 100-Mbps segment based on its port speed.

Auto Negotiate: The speed is detected and the duplex mode is forced to half duplex.

Force 10 - TP: The port speed is forced to 10 Mbps.

Force 100 - TP: The port speed is forced to 100 Mbps.

Link Status Change Notify

The link status change notify state (No Change/Disable/Enable). When enabled, a trap will be sent to the receiver when a link status of the port has changed.

Enable: The trap is sent.

Disable: The trap is not sent.

Port Configuration Using Java Applet

Figure 5-23 shows that a port can be configured by clicking on the right mouse button followed by clicking on the left mouse button.

Figure 5-23 Configuring a Port

Bridge Module Control/Status

Selecting this option displays the Bridge Module Control/Status Menu as shown in Figure 5-24.

Figure 5-24 Bridge Module Control/Status Menu

The bridge module has two internal and one external bridge ports. The two internal ports bridge the 10/100 Ethernet Stackable Hub's 10-Mbps segment and 100-Mbps segment. The external port is used to bridge external devices.

To configure the bridge module:

Step 1. Select a 10/100 Ethernet Stackable Hub from the Group Number pull-down menu.

Step 2. Select **Submit**, to load the configuration for the selected hub.

Step 3. Make the appropriate configurations in the New Configurations panel.

Step 4. Select **SAVE** to update the module's new configuration.

Group Number

The ID number of the current 10/100 Ethernet Stackable Hub 8245 (1 to 6).

Description

Description of the slide-in module currently installed (read only).

External Port Interface Type

Description of the external port, for example RJ-45.

External Port Link Status

The current link status of the installed module. Read only (link up or link down).

External Port Speed

The module's external port speed (read only).

Hardware Status

Read-only description of the hardware status.

External Function Admin State

You can enable or disable the external bridge function.

Internal Function Admin State

You can enable or disable the internal bridge function if the hardware DIP switches are enabled. See "Installing an Optional Module" on page 2-7.

Enable: Enables the internal bridge function. The internal hardware DIP switch must also be enabled for the internal bridge to function.

Notes:

1. The internal bridge must be enabled in hardware with the DIP switch settings before the Admin state can be enabled. See Figure 2-4 on page 2-8 and Figure 2-5 on page 2-8.
2. If you have a stack of all manageable units (no managed units), you only need to set the bridge module's hardware DIP switch to enable it to act as an internal bridge.

Disable: Disables the internal bridge function when the internal hardware DIP switches have been enabled. Once the internal bridge function is disabled, you must enable it to restore internal bridge operation.

The default value is Disable.

Notes:

1. These modules are not hot-swappable. You must remove power- from the 8245 before installing or removing bridge modules.
2. You should enable the internal bridge on only one bridge module when you have multiple bridge modules installed in a stack. This prevents a network loop condition.

Link Status Change Notify

When enabled, a trap will be sent to the receiver when link status of the port has changed.

Enabled: A trap is sent to the trap receivers if the link status changes.

Disabled: No trap is sent.

You can either enter into the Web page and make your configurations directly on the menu, or click on the module on the Java Applet with the right mouse button and then create your configuraton by clicking on Config with the left mouse button.

External AUI Module Control/Status

Selecting this option displays the External AUI Module Control/Status Menu as shown in Figure 5-25.

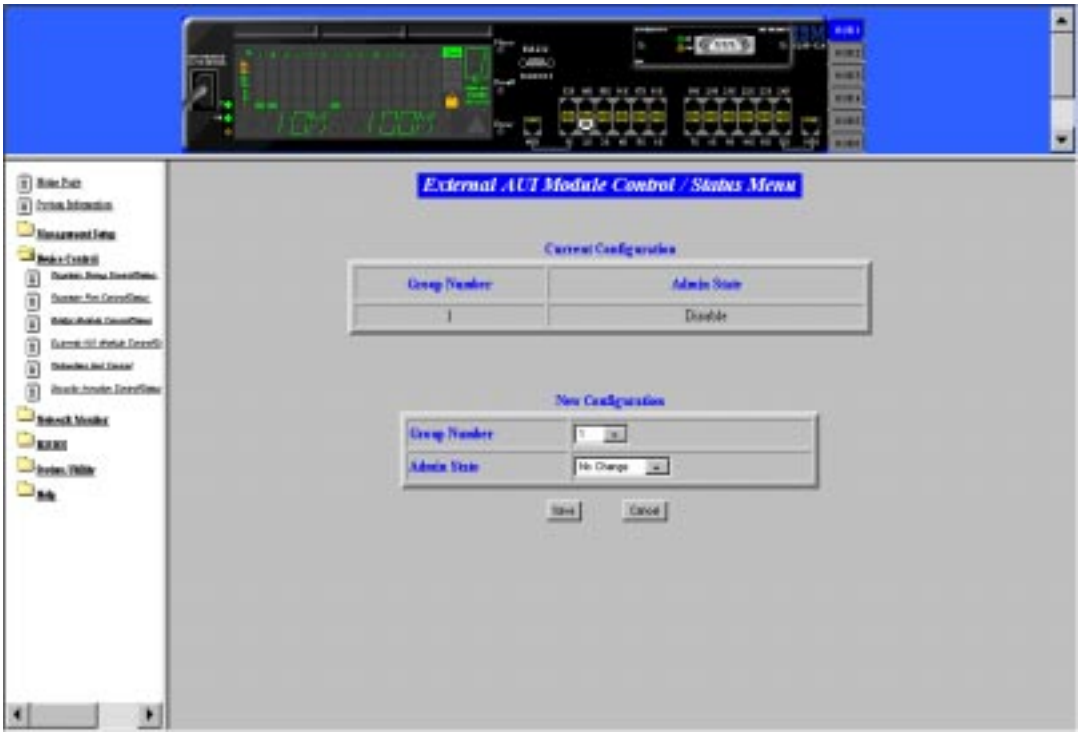


Figure 5-25 External AUI Module Control/Status Menu

The external AUI module is used to connect AUI devices to the 10/100 Ethernet Stackable Hub 8245. The AUI module is an external bridge and does not have an internal 10/100 bridge.

Group Number

A 10/100 Ethernet Stackable Hub ID in the stack (1 to 6).

Admin State

Enable or disable the AUI port operation.

To configure the AUI module, enter into the Web page and make your configurations directly on the menu, or click on the module on the Java applet with the right mouse button, and then create your configurations by clicking on **Config** with the left mouse button.

Redundant Link Control

Selecting this option displays the Redundant Link Control Menu as shown in Figure 5-26.

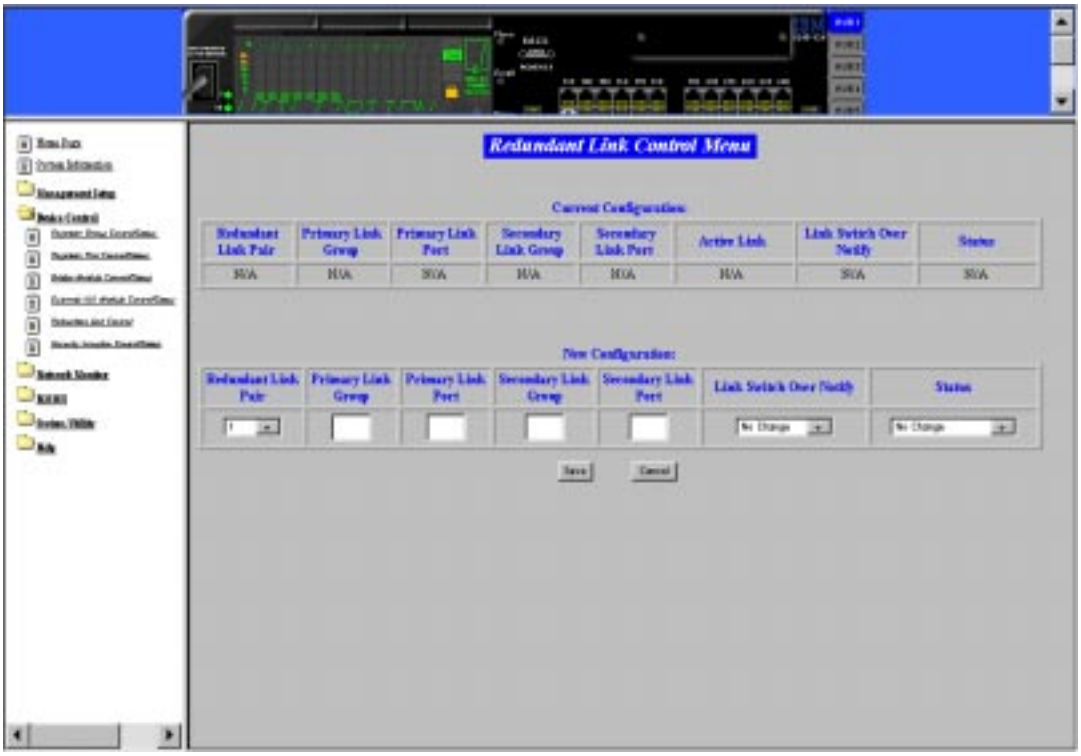


Figure 5-26 Redundant Link Control

The Redundant Link Control menu allows you to configure up to 18 pairs of redundant links. A redundant pair consists of any two physically linked ports in the 10/100 Ethernet Stackable Hub 8245 stack, where one is the primary link port and the other is a secondary link port. The primary link is the *active* link between two devices and the secondary is a backup and is set to *inactive* to prevent looping. If the primary link fails, the secondary link becomes active. The secondary link stays active even if the primary link recovers. You must manually reset the primary link status to active in order to re-instate the redundant pair.

You can configure a primary link by assigning a specific port on a specific hub to a Link Pair Index. You can assign a secondary link by assigning a specific port on a specific hub to the same Link Pair Index.

Redundant Link Pair

Index number for a linked pair (1 to 18).

Primary Link Group

This object identifies the Hub ID number of a primary link for a given redundant link pair.

Primary Link Port

This object identifies the port number of a primary link for a given redundant link pair.

Secondary Link Group

This object identifies the Hub ID of a secondary link for a given redundant link pair.

Secondary Link Port

This object identifies the port number of a secondary link for a given redundant link pair.

Active Link

This object indicates the current status for a given redundant link pair.

Primary: The port is the currently the active primary link.

Secondary: The port is currently the secondary port.

Both fail: The secondary link port is the active link and it has failed. To reinstate the link pair set the link pair status to **enable**.

Link Switchover Notify

If the link status of active link is “down” for more than 5 seconds, then the *active link failed* is detected and *port switchover* is performed and a trap is sent to the trap receivers.

Enable

A trap is sent to the trap receivers.

Disable

A trap is not sent to the trap receivers.

Status

You can **enable, disable** or **suspend** the operation of specific redundant link pairs:

Enable

The redundant link pair is in the normal operation mode. The primary port is active and the secondary port is disabled.

Disable

If you disable the primary port, the status of this link pair is changed to the *suspend state* and indicates that the active port has been disabled and the redundant link function is temporary suspended. If you enable the primary port later on, the status of this redundant link pair is changed to *enabled*.

If you disable the secondary port, the status of this link pair is changed to the *suspend* state and both ports are disabled. If you enable the secondary port later on, the status of this link pair is changed to enabled and the redundant link pair is in the normal operation mode.

Notes:

1. Setting the redundant link to disable does not cause the ports to be switched over.
2. Redundant link pairs must have Link Test enabled.

Return-to-primary

Selecting this option and pressing **Enter** reassigns the primary link as active link again. A trap is sent to the trap receivers if the status of the redundant link is *enable*. If the status is *suspend* then the link pair is reactivated but no trap is sent.

Suspend

Indicates that the active ports are disabled and the redundant link function is temporarily suspended until you set its state to *enable*.

Note: The suspend state does not cause the port to be switched over.

To add or edit a Redundant Link Pair:

Step 1. Select a Redundant Link Pair Index from the pull down menu.

Step 2. Enter **Group**, **Port**, **Link Switch Over Notify**, and **Status Information**.

Step 3. Select **SAVE**. The information becomes effective immediately.

Security Intrusion Control/Status

Selecting this option displays the Security Intrusion Control/Status Menu as shown in Figure 5-27 and Figure 5-28 on page 5-47.

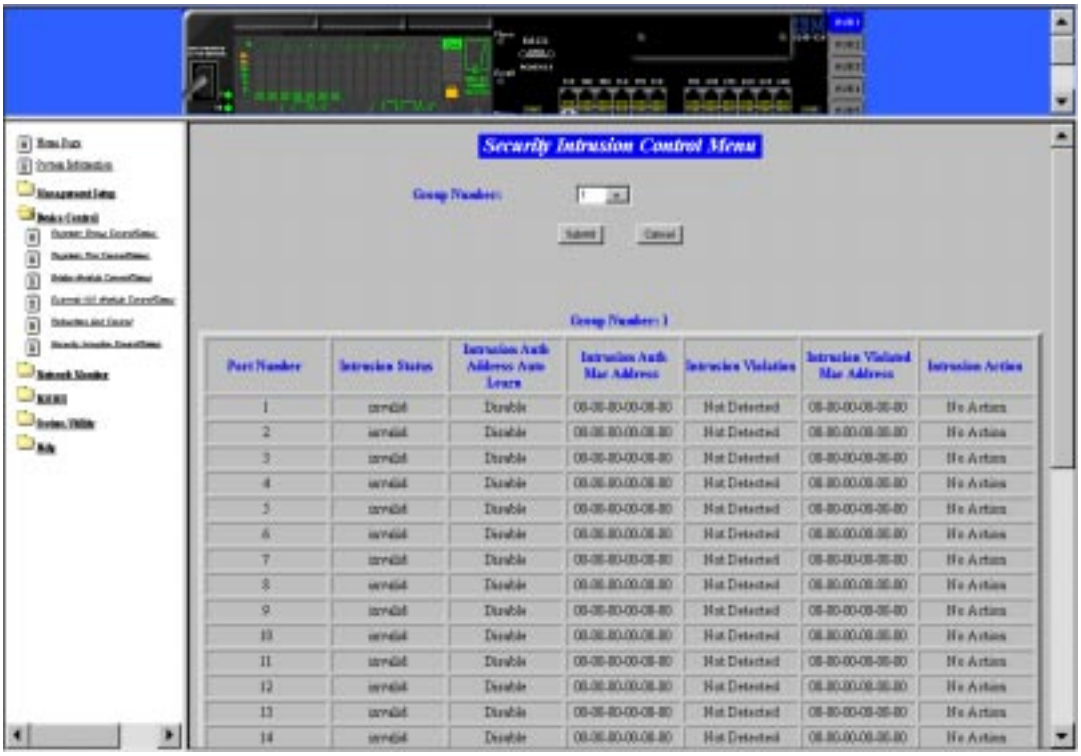


Figure 5-27 Security Intrusion Control/Status Menu (Top/Upper View)

The intrusion control enables you to set up secure ports that either allow access by a single authorized MAC address or allow different actions to be taken when accessed by any IP address other than the authorized IP address. These actions could include sending traps or partitioning the port or both.

Group Number

The Group Number is used to specify a hub range (1 to 6).

Port Number

Specifies to port number of a hub (1 to 12/24).

Intrusion Status

Enable: The security intrusion control for the port is enabled.

Disable: The security intrusion control for the port is disabled.

Invalid: Purge the security intrusion control configuration for the current port from the system database.

Figure 5-28 Security Intrusion Control/Status Menu (Bottom/Lower View)

Intrusion Authentication Address Auto-Learn

Enable: The hub records the MAC address of the first device that the current port receives data from. The learn function is then disabled and the recorded MAC address is the authorized MAC address. This address is displayed in the Intrusion Authentication MAC address field.

Disable: Auto-learn operation is disabled.

Intrusion Authentication MAC Address

The MAC address of a device that is allowed to connect with this particular port.

Intrusion Violation

Detected: When an intrusion of an unauthorized MAC address occurs, the MAC address that caused the intrusion is written to the Intrusion Violated MAC Address field.

Not Detected: No intrusion has been detected.

Intrusion Violated MAC Address

Displays the MAC address of the last unauthorized device to contact this port.

Intrusion Action

The action that will be performed when the hub detects an intrusion.

No Action: No action will be taken.

Send Trap: A trap is sent to the trap receivers.

Partition: The port is partitioned.

Send Trap And Partition: The port is partitioned and a trap is sent to the trap receivers.

Note: If another hub or unrouted switch is attached to a port with Security Intrusion enabled, then only one of possibly many MAC address will be allowed to pass data.

To configure the security intrusion function, you can set up secure ports that allow access by single authorized MAC address from the Security Intrusion Control/Status Menu as the following steps:

Step 1. Enter **Group Number** and press **Submit** to get intrusion information on a hub.

Step 2. To add or edit intrusion on a port, select **Port Number** from the pull down menu.

Step 3. Enter **Intrusion Status, Auto Learn, MAC Address Information**, and **Caption**.

Step 4. Press **SAVE**. The information becomes effective immediately.

Network Monitor

This menu lets you monitor the network traffic and analyze the network utilization.

Repeater Statistics Information

Displays the total statistic counters for the 10-Mbps and 100-Mbps segments for all hubs in the stack.

Repeater Group Statistics Information

Displays the statistic counters for each hub.

Repeater Port Statistics Information

Displays the statistic counters for each port.

Address Tracking Information

Enables a network management application to passively gather information about which network addresses are connected to which ports of a hub.

Address Search Information

Active address tracking capability is used to watch for a given MAC address and report which port it was seen on.

Broadcast Storm Protection

Monitors the broadcast counters of each hub port to detect if the broadcast storming exists in the network.

Broadcast Storm Detected

Each hub port or optional module port which causes broadcast storm will be displayed.

Repeater Statistics Information

Selecting this option displays the Repeater Statistics Information Menu as shown in Figure 5-29.

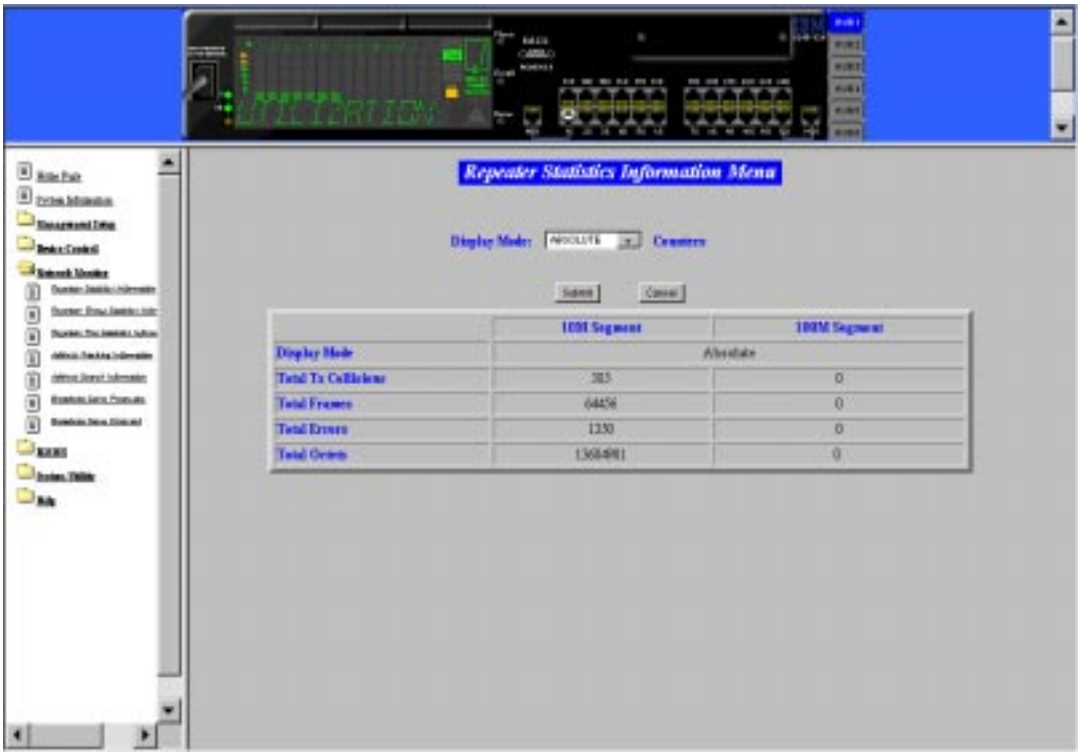


Figure 5-29 Repeater Statistics Information Menu

Display Mode

Enables you to display counters in either absolute mode or relative mode for the 10-Mbps and 100-Mbps segments for all hubs in the stack.

Absolute Mode: Select **ABSOLUTE** and select **SUBMIT**. Each counter will represent the value collected since the system started. You cannot reset the absolute counters.

Relative Mode: Select **RELATIVE** and select **SUBMIT**. Each counter will be reset to 0 and will then represent the value collected since you selected the relative mode. You can reset the relative counter to 0 by changing to Absolute Mode and then changing back to Relative Mode.

Total Tx Collisions

The number of transmission collisions that have occurred in this hub.

Total Frames

The number of frames of valid frame length that have been received on the ports of this stack segment and not including FCS Error and Collision Event.

Total Errors

Total errors received by the stack segment including FCS Errors, Align Errors, Frame Too Long, Short Events, Late Events, Very Long Events and Rate Mismatch.

Total Octets

The number of octets contained in the valid frames that have been received by this hub.

Repeater Group Statistics Information

Selecting this option displays the Repeater Group Statistics Information Menu as shown in Figure 5-30.

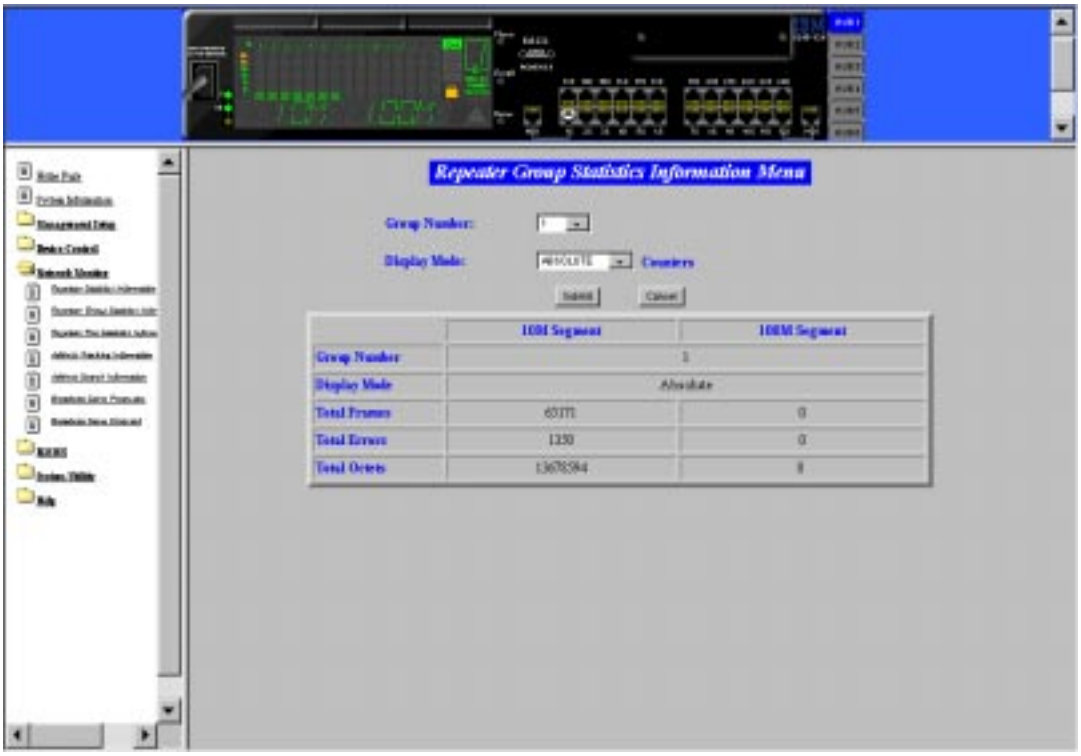


Figure 5-30 Repeater Group Statistics Information Menu

This menu displays statistics information counters for the current hub (group number). Counters are displayed in absolute or relative values by toggling the display mode. Absolute values represent the value collected since system started. You cannot clear absolute counters. Relative counters represent the values collected since the relatively mode was selected. You can reset the relative counters to 0 by changing to Absolute Mode and then changing back to Relative Mode.

Group Number

The ID number of a hub in a stack (1 to 6).

Display Mode

Displays counters in Absolute and Relative Mode.

Total Frames

The number of frames of valid frame length that have been received on the ports of this hub and not including FCS errors and collision events.

Total Errors

Total errors received by all of the ports of this hub. Errors include FCS Errors, Align Errors, Frame Too Long, Short Events, Late Events, Very Long Events and Rate Mismatch.

Total Octets

The total number of octets contained in the valid frames that have been received on the ports of this hub.

Repeater Port Statistics Information

Selecting this option displays the Repeater Port Statistics Information Menu as shown in Figure 5-31. It displays counter information for the current port of the current hub.

Figure 5-31 Repeater Port Statistics Information

To view port statistic counters:

Step 1. Select the Hub ID (Group Number) of the 10/100 Ethernet Stackable Hub 8245 to read from.

Step 2. Select a port.

Step 3. Select the display mode.

Step 4. Select **Submit** to load the port counter information for the port on the selected hub.

Group Number

The ID number of an 10/100 Ethernet Stackable Hub in a stack (1 to 6).

Port Number

Port number of the selected group (1 to 12/24).

Display Mode

Display counters in absolute or relative values.

Readable Frames

Total readable frames received by the port.

Readable Octets

Total readable octets received by the port.

FCS Errors

The total number of packets received by the port that had a bad Frame Check Sequence.

Alignment Errors

Total Alignment Error frames within the correct size (64 to 1518 octets) received by the port.

Frame Too Long

Total frames received by the port that were longer than 1518 octets (excluding framing bits, but including FCS octets).

Short Events

Total frames received by the port that were shorter than 64 octets or for which the activity duration was shorter than the event, ShortEventMaxTime (74 to 82 bit times).

Runts

The total number of packets received that were less than 64 octets due to collisions or for which the activity duration was greater than the ShortEventMaxTime event and less than the ValidPacketMinTime event.

Collisions

Total collisions on a port.

Late Events

Total events received by the port where the activity duration is greater than the LateEventThreshold.

Very Long Events

Total events received by the port where the activity duration is greater than the MAU Jabber Lockup Protection timer TW3.

Data Rate Mismatches

Total frames received by the port with no collisions and for which the activity duration was greater than the ValidPacketMinTime event and also the frequency (data rate) was detectable mismatched from the local frames mismatch frequency.

Auto Partitions

Total number of times the port was auto-partitioned.

Isolates (100M only)

Total isolates for 100-Mbps transmissions. This counter is incremented by one

each time that a port automatically isolates itself as a consequence of false carrier events. The conditions that cause a port to automatically isolate itself are defined by the transition from the False Carrier state to the Link Unstable state. The port will automatically recover.

Symbol Errors (100M only)

Total symbol errors for 100-Mbps transmissions. This counter is incremented by one for each valid length packet received at the port with at least one occurrence of an invalid data symbol. This can increment only once per valid carrier event.

Total Errors

Total errors received by the port including FCS Errors, Align Errors, Frame Too Long, Short Events, Late Events, Very Long Events and Rate Mismatch.

Broadcast Packets

Total broadcast packets received by the port.

Multicast Packets

Total multicast packets received by the port

Address Tracking Information

Selecting this option displays the Address Tracking Information Menu as shown in Figure 5-32.

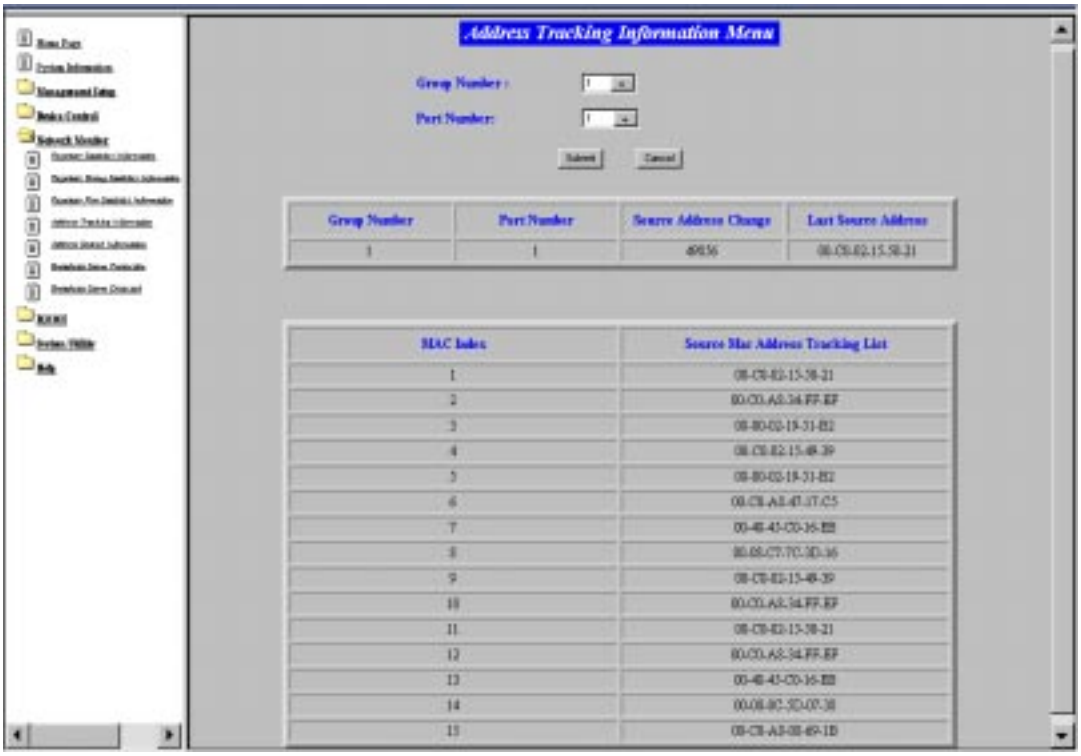


Figure 5-32 Address Tracking Information Menu

The 10/100 Ethernet Stackable Hub 8245 provides per-port address (MAC address-based) tracking capability. The address-tracking function records the source MAC of each data packet and provides the filters for data analysis.

Group Number

The ID number of a hub in a stack.

Port Number

Port number of the selected hub (1 to 12/24).

Source Address Change

This counter is incremented by one for each time that the Last Source Address for this port has changed. This indicates whether a link is connected to a single device or another multi-user segment. The approximate minimum time for rollover of this counter is 81 hours.

Last Source Address

Indicates the source MAC address of the last readable frame received by this port. If this port has received no frames since the hub began monitoring the port activity, a null string will be displayed.

MAC Index of Address Tracking Information of Web-based Management

The MAC index is used to indicate the ordering of source MAC address seen on the port.

Source MAC Address Tracking List

A list of source MAC addresses that were recently received on this port. The first source MAC address (00-40-AC-1C-80-23 for example) in the tracking list contains the value that is given by the Last Source Address for this port. This list can contain 15 entries. The first entries are deleted to accommodate new entries when the list is full.

Address Search Information

Selecting this option displays the Address Search Information Menu as shown in Figure 5-33.

Figure 5-33 Address Search Information Menu

You can use the active address search capability to watch for a given MAC address and report which port it was seen on. You can also use it to collect the necessary information for mapping the topology of a network. Up to eight MAC address can be searched simultaneously.

Search Index

Identifies the index of the source address to be searched in the system for which this entry contains information (1 to 8).

Address Searched

Identifies the source address to be searched in the system for which this entry contains information.

Address Search Lock

Used by a management station as an advisory lock for a search entry. The search lock will increment by 1 up to 2^{32}-1.

Address Search Status

In Use: A management station has obtained ownership.

Not In Use: No other management station has obtained ownership.

A management station first retrieves the values of the appropriate instances of the Address Search Lock and Address Search Status objects, periodically repeating the retrieval if necessary, until the value of Address Search Status is *Not In Use*. The management station then tries to set the same instance of the Address Search Lock object to the value it just retrieved, the same instance of the Address Search Status object to *In Use*, and the corresponding instance of Address Search Owner to a value indicating itself. If the set operation succeeds, then the management station has obtained ownership of the entry and the value of Address Search Lock is incremented by the agent. Failure of the set operation indicates that some other manager has obtained ownership of the entry.

Address Search State

The current state of the MAC address search on this hub (None, Single, or Multiple).

Note: The result of address search for a given Source MAC Address is represented by **Address Search State, Address Search Group,** and **Address Search Port**.

- Source MAC Address is detected on a port: Address Search State is set to **Single,** (Address Search Group, Address Search Port) shows the detected port number.
- Source MAC Address is detected on multiple ports: Address Search State is set to **Multiple,** (Address Search Group, Address Search Port) shows the port number, which detects the given Source MAC Address first.
- Source MAC Address is not detected on any port: Address Search State is set to **None,** (Address Search Group, Address Search Port) is undetermined.

Address Search Group

The group Hub ID received, whose source address corresponds to the address searched (1 to 6).

Address Search Port

The received port number whose source address corresponds to the address searched (1 to 12/24).

Address Search Owner

The management capability which currently has “ownership” of this search entry (Web).

The owner for a given address search entry could be one of the following:

CONSOLE: If the entry is locked by the local console or Remote Telnet, the owner is CONSOLE.

WEB: If the entry is locked by the Web-based manager, the owner is WEB.

hubrptrAddrSearchOwner: If the entry is locked by the SNMP manager, the owner will be given by the SNMP manager by setting the MIB object hubrptrAddrSearchOwner.

To perform an address search:

Step 1. Enter an index number in the Search Index field at the bottom of the Address Search Information Menu (1 to 8).

Step 2. Type in the source MAC address to be searched.

Step 3. Set Address Search Status to **In-Use**.

Step 4. Select **SAVE** to get the owner of this entry. If the entry is free and available, the Address Search Lock will be increased by 1, the Address Search Status will be set to “In Use” and the Address Search Owner will be set to “Web.” Otherwise the request to own the entry will be rejected.

Step 5. Repeat steps 1 through 4 for all addresses to be searched.

Broadcast Storm Protection

Selecting this option displays the Broadcast Storm Protection Menu as shown in Figure 5-34.

Figure 5-34 Broadcast Storm Protection

The 10/100 Ethernet Stackable Hub 8245 periodically monitors the broadcast counters of each hub port to detect a broadcast storm condition. The hub port that causes the broadcast storm can be automatically partitioned, or a trap can be sent to the trap receivers, or both. The 10/100 Ethernet Stackable Hub 8245 continually monitors those ports that have been partitioned to check if the broadcast storm condition still exists. The port will be permanently partitioned if the broadcast storm does not subside with 2 minutes.

You can configure the broadcast threshold value for each port, each segment, and each optional module. The Segment Rate Threshold, Port Rate Threshold, and Optional Module Rate Threshold determines whether the broadcast storm exists or not.

Segment ID

Specifies the segment where the broadcast storm protection function is applied (10-Mbps or 100-Mbps segment).

Segment Rate Threshold

The number of broadcast packets received on a given segment per second. The range is 0 to 14,880 packets per second.

Optional Module Rate Threshold

The number of broadcast packets received on each uplink of a given optional module per second. The range is 0 to 14,880 packets per second.

Port Rate Threshold

The number of broadcast packets received on a given port per second. The range is 0 to 14,880 packets per second.

Alarm Action

Once broadcast storm is detected on a given port, segment, or uplink port, the Alarm Detection Status will be set to *Detected*, and the correct action shall be performed based on the value specified by its Broadcast Alarm Action

Partition: The port will be disabled. Once a port is partitioned due to a broadcast storm, the Broadcast Storm protection function will continue to monitor the port. The port is disabled for 15 seconds and re-enabled for 5 seconds. This process is repeated for 2 minutes. If the broadcast storm still exists, the port is disabled and no longer monitored.

Note: You must enable the port once the source of the broadcast storm has been handled. You should resolve the broadcast storm before re-enabling the port.

Send Trap and Partition: The port will be disabled and a trap will be sent.

Sent Trap: The trap will be sent.

None: No action will be taken.

Alarm Status

Enabled: Enables the broadcast monitoring and protection function on this segment.

Disabled: Disables the broadcast monitoring and protection function on this segment.

Invalid: Purges the broadcast monitoring and protection setting for this segment.

Formula for calculating broadcast packet rate

$$\text{Broadcast packet rate} = \frac{\text{Broadcast packet received}}{\text{Seconds}}$$

Configuring Broadcast Storm Protection

To detect the broadcast storm of the 10/100 Ethernet Stackable Hub, you have to configure the following parameters from the Broadcast Storm Protection Menu:

Step 1. Select **100 Mbps Segment** from Segment ID field.

Step 2. Configure **Segment Broadcast Packet Rate Threshold**.

Step 3. Configure **Optional Module Broadcast Packet Rate Threshold**.

Note: The **Optional Module Broadcast Packet Rate Threshold** of 100 Mbps segment is used for both 10 Mbps and 100 Mbps Broadcast Storm Detection.

Step 4. Configure **Broadcast Alarm Action**.

Step 5. Enable the broadcast storm protection function.

To detect the broadcast storm of the AUI module, the users have to configure the following parameters from the Broadcast Storm Protection Menu:

Step 1. Select **10 Mbps Segment** from **Segment ID** field.

Step 2. Configure **Segment Broadcast Packet Rate Threshold**.

Step 3. Configure **Optional Module Broadcast Packet Rate Threshold**.

Note: The **Optional Module Broadcast Packet Rate Threshold** of 10 Mbps segment is used for AUI module Broadcast Storm Detection.

Step 4. Configure **Broadcast Alarm Action**.

Step 5. Enable the broadcast storm protection function.

Broadcast Storm Detected

Selecting this option displays the Broadcast Storm Detected Menu as shown in Figure 5-35.

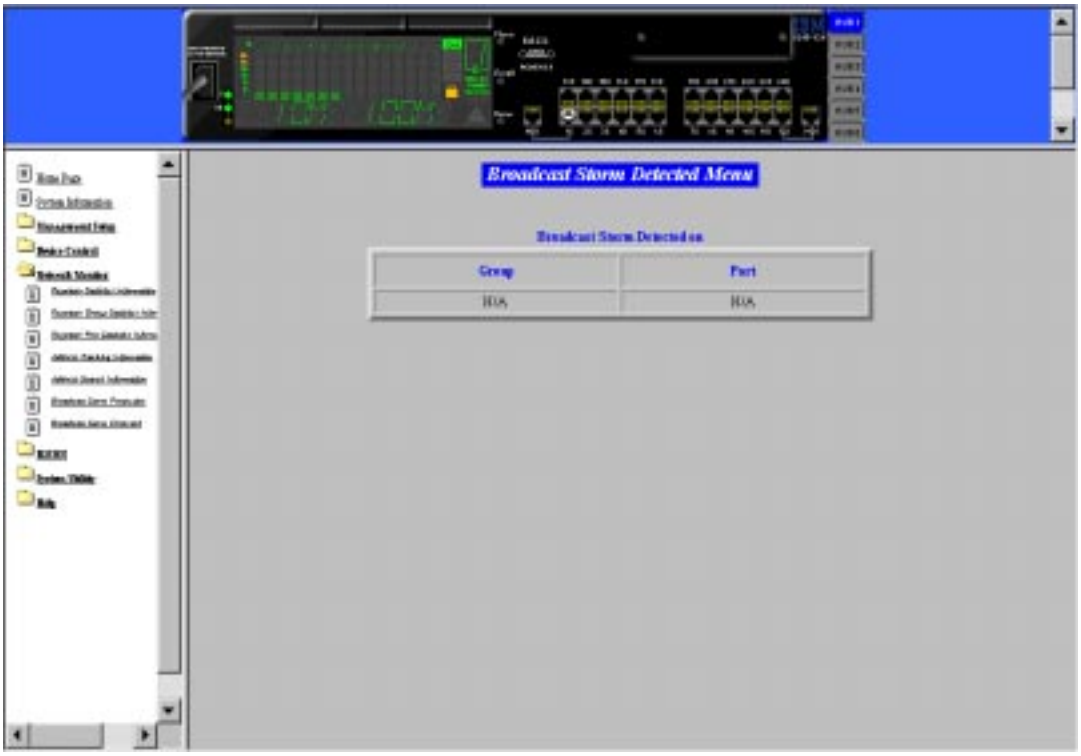


Figure 5-35 Broadcast Storm Detected Menu

When a broadcast storm is detected, the hub and port, segment or uplink port that are causing the storm will be listed in the Broadcast Storm Detected Menu. If no broadcast storm is detected, this menu displays N/A under Group and Port.

RMON

The Remote Monitoring MIB (RMON) allows you to monitor LANs remotely.

Selecting this option displays the following menus:

RMON Statistic Group Configuration

Configures hub data source.

RMON History Group Configuration

Configures history groups.

RMON Alarm Group Configuration

Configures alarm groups.

RMON Event Group Configuration

Configures event groups.

RMON Statistics Information

Displays statistics information by index.

RMON History Information

Displays history information by index.

RMON Event Log

Displays event log by index.

RMON Statistics Group Configuration

Selecting this option displays the RMON Statistics Group Configuration Menu as shown in Figure 5-36.

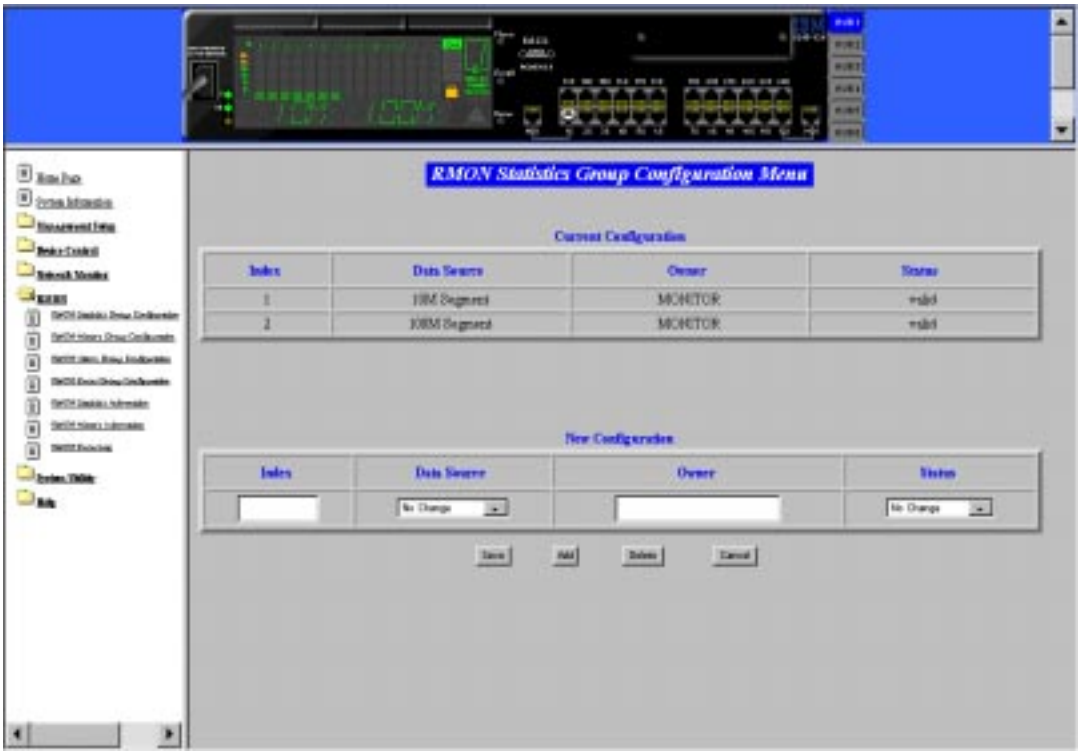


Figure 5-36 RMON Statistics Group Configuration Menu

The RMON Statistics Group Configuration Menu displays current group settings and provides new configuration entry fields.

To create a new entry of RMON statistics from the RMON Statistics Group Configuration Menu:

Step 1. Go to New Configuration.

Step 2. Type in a new index value to the Index field.

Step 3. Select **10M Segment** or **100M Segment** from the Data Source field.

Step 4. Type the owner's name in the owner field.

Step 5. To enable, select **Valid** from the Status Menu, otherwise it will appear as UnderCreation.

Step 6. Select **Add** to create a new entry.

Statistics Group Index

A value from 1 to 65535. The value must be unique. Not to be confused with Data Source Index.

> **Data Source Index:** "This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 1213 and RFC 1573[4,6] for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1."

Data Source

Displays the data source as segment 10-Mbps/100-Mbps or no change.

Owner

Displays the owner of the statistics. The owner is always the monitor.

Status

Displays the current status of each port.

> **Valid:** An entry is fully configured and consistent.
>
> **underCreation:** Entry is in the process of being created and can be incomplete. If an entry is valid, the entry should be made under-Creation to be modified.
>
> **invalid:** Entry is cleared.

Table 5-1 RMON Statistics Group Configuration Menu Button Selection

Add	To create a new entry
Save	To update an existed entry with Status value set to UnderCreation
Delete	To delete an existing entry
Cancel	To cancel the configuration change

RMON History Group Configuration

Selecting this option displays the RMON History Group Configuration Menu as shown in Figure 5-37.

Figure 5-37 RMON History Group Configuration Menu

This menu provides a means of correlating the data gathered by the statistics group over time. It records statistical samples according to the user-specified time interval and duration and stores them for later retrieval.

Notes:

1. Selecting **Save** updates an existing entry with Status value set to UnderCreation.
2. Selecting **Add** creates a new entry.

To create a new entry of RMON history from the RMON History Group Configuration Menu:

Step 1. Go to New Configuration.

Step 2. Type in a new index value to the Index field.

Step 3. Select **10 M Segment** or **100 M segment** from the Data Source field.

Step 4. Type in the number of buckets requested.

Step 5. Type in the interval in seconds between buckets.

Step 6. Type owner's name to the Owner field.

Step 7. To enable, select **Valid** from the Status menu, otherwise it will appear as UnderCreation.

Step 8. Select **Add** to create a new entry.

History Group Index

A value from 1 to 65535. The value must be unique. Not to be confused with Data Source Index.

> **Data Source Index:** "This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 1213 and RFC 1573[4,6] for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1."

Data Source

Displays the data source as segment 10-Mbps or 100-Mbps. The default is 10 Mbps.

Bucket requested

Number of sample buckets you want to collect and store. The range is 1 to 65535. The default is 50 buckets.

Bucket granted

Number of sample buckets that will be collected and stored. The number granted is affected by available resources.

Interval

Interval in seconds between bucket samples. The range of the interval is 1 to 3600 seconds (1 hour). The default is 1800 seconds.

Owner

The entity that configured this entry and is using the resources assigned to it. A string of up to 12 characters.

Status

A valid status has all fields filled in. Setting the status to invalid deletes the index. An index with incomplete information in some fields automatically sets the status as **underCreation**.

Valid: An entry is fully configured and consistent.

underCreation: An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified.

Invalid: Entry is cleared.

Table 5-2 RMON History Group Configuration Menu Button Selection

Add	To create a new entry
Save	To update an existed entry with Status value set to UnderCreation
Delete	To delete an existing entry
Cancel	To cancel the configuration change

RMON Alarm Group Configuration

Selecting this option displays the RMON Alarm Group Configuration Menu as shown in Figure 5-38.

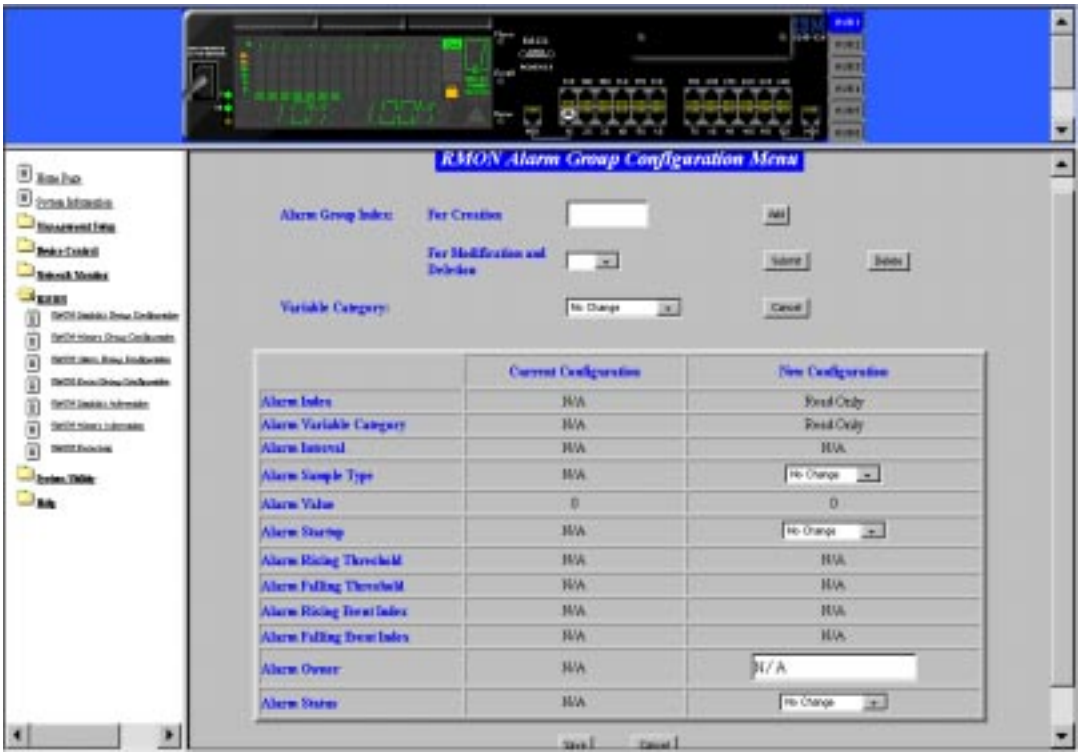


Figure 5-38 RMON Alarm Group Configuration Menu

You can create up to 16 alarm control entries through the Web-based manager or an SNMP manager. The Alarm Group is used to track extraordinary events or activities. It enables you to set the RMON alarms to specific thresholds. When the traffic volume exceeds or drops below those thresholds, an event is activated. A rising threshold is used to monitor the value of a tracked variable when it rises above a particular level. A falling threshold is used to monitor the value of a tracked variable when it falls below a particular level. Thresholds can be set against either an absolute value or a delta (change in) value. Alarms can generate an action response through the Events Group.

Creating a New Alarm Control Entry

Use the following procedures to create a new alarm control entry:

Step 1. Go to RMON Alarm Group Configuration Menu.

Step 2. Create a new entry first by using the following steps:

a. Go to **Alarm Group Index** and type the index number in the **For Creation** field to select a new index.

b. Select one of the variable categories from the **Variable Category** fields:

RMON: The alarm variable will be one of the RMON Ethernet Statistics counters, as specified by RFC1757 RMON.

Repeater Group: The alarm variable will be one of the group counters specified by RFC1516 Repeater MIB (for 10-Mbps segments only).

Repeater Port: The alarm variable will be one of the port counters specified by RFC1516 Repeater MIB (for 10-Mbps and 100-Mbps segment common counters only).

c. Select **Add**. A new entry will be created based on the variable category with a default value.

Step 3. Go to **New Configuration** area and type in the following configuration data for a new entry:

- **Alarm Interval**
- **Group ID**
- **Counter ID:** Specifies the particular counter ID of a given variable category to be sampled in Total Frames/Total Octets/Total Errors.
  - For RMON variable, select a counter from the Counter ID field.
  - For Repeater Group variable, select the group number from Group Number field and select a counter from the Counter ID field.
  - For Repeater Port variable, select the group/port number from Group/Port Number field and select a counter from the Counter ID field.
- **Alarm Sample Type**
- **Alarm Startup**
- **Alarm Rising Threshold**
- **Alarm Falling Threshold**
- **Alarm Rising Event Index**
- **Alarm Falling Event Index**
- **Alarm Owner (12 characters)**
- **Alarm Status (underCreation and Valid)**

Step 4. Select **Save** command.

To update an existing Alarm Control entry:

Step 1. Select an existing index from the list box “For Modification and Deletion”.
Step 2. Select **Submit** for modificaiton or select **Delete** to delete the entry.
Step 3. Modify the contents on the table if Submit is selected.

Alarm Index

A value from 1 to 65535. The value must be unique. Not to be confused with Data Source Index.

> **Data Source Index:** “This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 1213 and RFC 1573[4,6] for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1.”

Alarm Variable Category

RMON: An RMON Ethernet Statistics counter.

Repeater Group: A group counter specified by RFC1516 repeater MIB for 10-Mbps segments only.

Repeater Port: A port counter specified by RFC1516 repeater MIB for 10-Mbps and 100-Mbps segments common counters only.

Alarm Interval

Time in seconds over which the data is sampled for each bucket. The range is 1 to 3600 seconds (1 hour). The default is 1800 seconds.

Group ID

Shows an index of the Ether Statistics entries created (maximum of 16 entries).

Note: Default values are 1 for 10-Mbps segment, and 2 for 100-Mbps segments.

Alarm Sample Type

Absolute: Value stored is compared directly to the threshold level.

Delta: The value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the threshold value.

Alarm Startup

Of rising and falling thresholds, the one that must be crossed first for an event to be generated.

Rising Alarm: Event is generated when the rising threshold is crossed first.

Falling Alarm: Event is generated when the falling threshold is crossed first.

Both Alarm: Event is generated when either the rising or falling threshold is crossed first.

Alarm Rising Threshold

Threshold for the sampled statistic. When the current sampled value is ***greater than or equal to*** this threshold, and the value of this sample at the last sampling interval was ***less than*** the threshold, then a single event is generated.

After a rising event is generated, another rising event is not generated until the sampled value falls below this threshold and reaches the falling threshold.

Alarm Falling Threshold

Threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value of this sample at the last sampling interval was greater than the threshold, then a single event is generated. After a falling event is generated, another falling event is not generated until the sampled value rises above this threshold and reaches the rising threshold.

Alarm Rising Event Index

Index of the event entry that this Index used when the rising threshold is crossed. It must coincide with the Event Group Index. The range is 0 to 65535. If you choose 0, no event is generated when this threshold is met.

Alarm Falling Event Index

Index of the event entry that is used when the falling threshold is crossed. It must coincide with the Event Group Index. The range is 0 to 65535. If you choose 0, no event is generated when this threshold is met.

Alarm Owner

Text field to identify the owner.

Alarm Status

valid: An entry is fully configured and consistent.

underCreation: An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified.

invalid: Entry is cleared.

Table 5-3 RMON Alarm Group Configuration Menu Button Selection

Save	To update an existed entry with Status value set to UnderCreation
Cancel	To cancel the configuration change

RMON Event Group Configuration

Selecting this option displays the RMON Event Group Configuration Menu as shown in Figure 5-39.

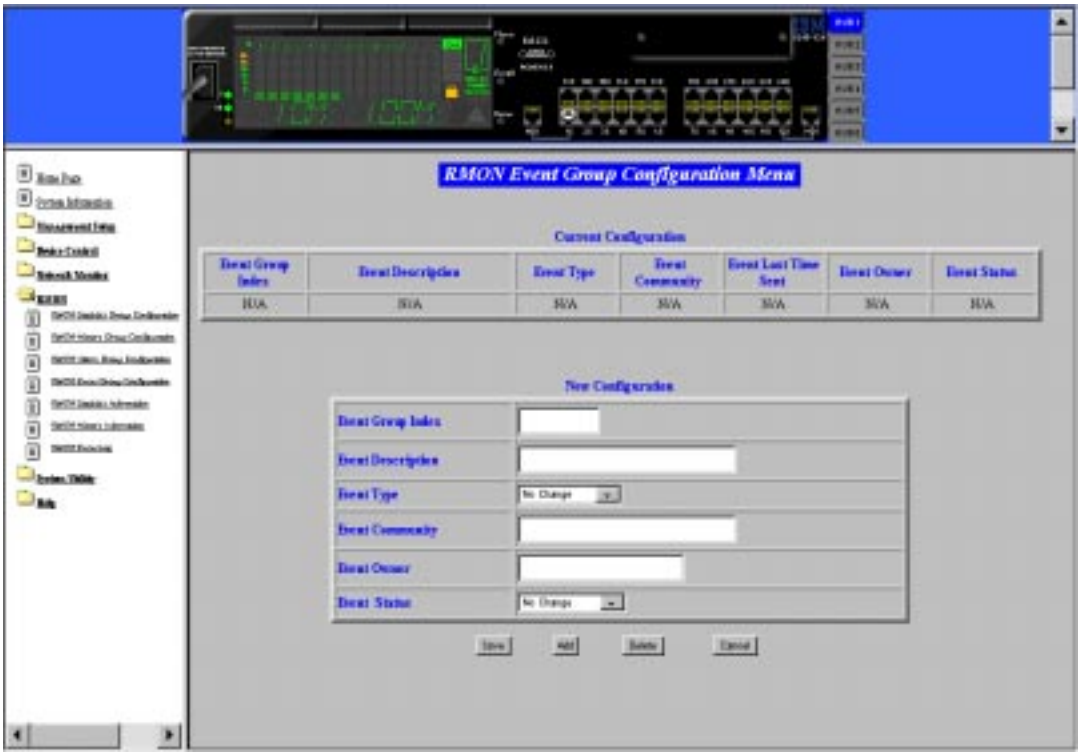


Figure 5-39 RMON Event Group Configuration Menu

You can create up to 32 alarm control entries through the Web-based manager or an SNMP manager.

To create a new entry of RMON event from the RMON Event Group Configuration Menu:

Step 1. Go to New Configuration.

Step 2. Type in a new index value to the Event Group Index field.

Step 3. Type in optional Event Description.

Step 4. Select **Event Type** from the menu.

Step 5. Type in the Event Community name.

Step 6. Type owner's name to the Owner field.

Step 7. To enable, select **Valid** from the Status menu, otherwise it will appear as UnderCreation.

Step 8. Select **Add** to create a new entry.

Event Group Index

A value from 1 to 65535. The value must be unique. Not to be confused with Data Source Index.

> **Data Source Index:** "This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 1213 and RFC 1573[4,6] for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1."

Event Description

A comment that describes this event.

Event Type

None: No Action will be taken.

Log: When an alarm occurs, the alarm status will be logged.

Trap: When an alarm occurs, a trap will be sent to the specified SNMP community.

Log and Trap: When an alarm occurs, the alarm status will be logged and a trap will be sent to the specified SNMP community.

Event Community

A string that specifies the SNMP community to which an SNMP trap is to be sent (up to 16 characters).

Event Last Time Sent

The value of System Up Time at the time this event entry last generated an event.

Event Owner

Text field to identify the owner (up to 12 characters).

Event Status

Valid: An entry is fully configured and consistent.

Under Creation: An entry is in the process of being created and may be incomplete. If an entry is valid, the entry should be made underCreation to be modified.

Invalid: Entry is cleared.

Event None: No action will be performed.

Table 5-4 RMON Event Group Configuration Menu Button Selection

Add	To create a new entry
Save	To update an existed entry with Status value set to UnderCreation
Delete	To delete an existing entry
Cancel	To cancel the configuration change

RMON Statistics Information

Selecting this option displays the RMON Statistics Information Menu as shown in Figure 5-40.

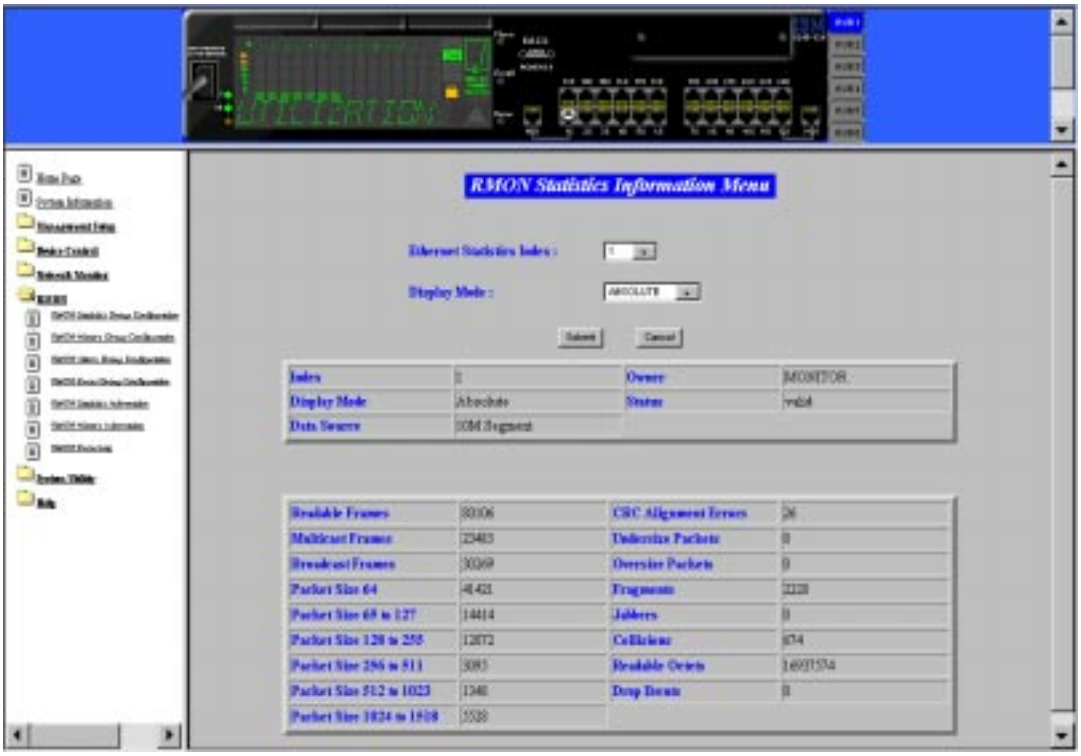


Figure 5-40 RMON Statistics Information Menu

An Ethernet statistics entry contains a collection of statistics (counters) kept for a particular Ethernet interface.

Data Source

Displays the data source as segment 10 Mbps or 100-Mbps.

Owner

Displays the owner of the statistics. The owner is always the monitor.

Status

Displays the current status of each port.

Valid: An entry is fully configured and consistent.

underCreation: Entry is in the process of being created and can be incomplete. If an entry is valid, the entry should be made under-Creation to be modified.

Invalid: Entry is cleared.

Ethernet Statistics Index

The value of the Ethernet Statistics Index uniquely identifies an Ethernet Statistics entry.

Display Mode

Displays counters for the 10 Mbps and 100Mbps segment for all hubs in the stack.

Absoluet Mode: Select **Absolute Display Mode** and select **Submit**. Each counter will represent the value collected since system start. The user cannot clear absolute counters.

Relative Mode: Select **Relative Display Mode** and select **Submit**. Each counter will be cleared to 0, and then represents the value collected since the relative mode was selected. You can reset the relative counters to 0 by changing to Absolute Mode then change back to Relative Mode.

Readable Frames

A whole number representing the number of readable frames received by the port.

Multicast Frames

Total number of good packets directed to this port, not including packets directed to the broadcast address.

Broadcast Frames

The total number of packets transmitted that were directed to the broadcast address. Does not include packets directed to multicast address.

Packet Size 64

The number of packets received that were 64 octets.

Packet Size 65 to 127

The number of packets received that were between 65 to 127 octets.

Packet Size 128 to 255

The number of packets received that were between 128 to 255 octets.

Packet Size 256 to 511

The number of packets received that were between 256 to 511 octets.

Packet Size 512 to 1023

The number of packets received that were between 512 to 1023 octets.

Packet Size 1024 to 1518

The number of packets received that were between 1024 to 1518 octets.

CRC Alignment Errors

The total CRC or alignment error frames within the proper size (64 to 1518 octets).

Undersize Packets

The number of packets received that were less than 64 octets long and were otherwise well formed.

Oversize Packets

The number of packets received that were longer than 1518 octets and were otherwise well formed.

Fragments

The total number of packets that were received that were longer than 1518 octets and had an FCS or alignment error.

Jabbers

The number of packets received that were less than 64 octets and had an FCS or alignment error.

Collisions

The number of collisions.

Readable Octets

The total number of octets of data, including bad packets and FCS octets, received on the hub and excluding framing bits.

Drop Events

The number of events in which packets were dropped by the monitor due to lack of resources.

RMON History Information

Selecting this option displays the RMON History Information Menu as shown in Figure 5-41. You can also refer to “RMON History Group Configuration” on page 5-69 for further information.

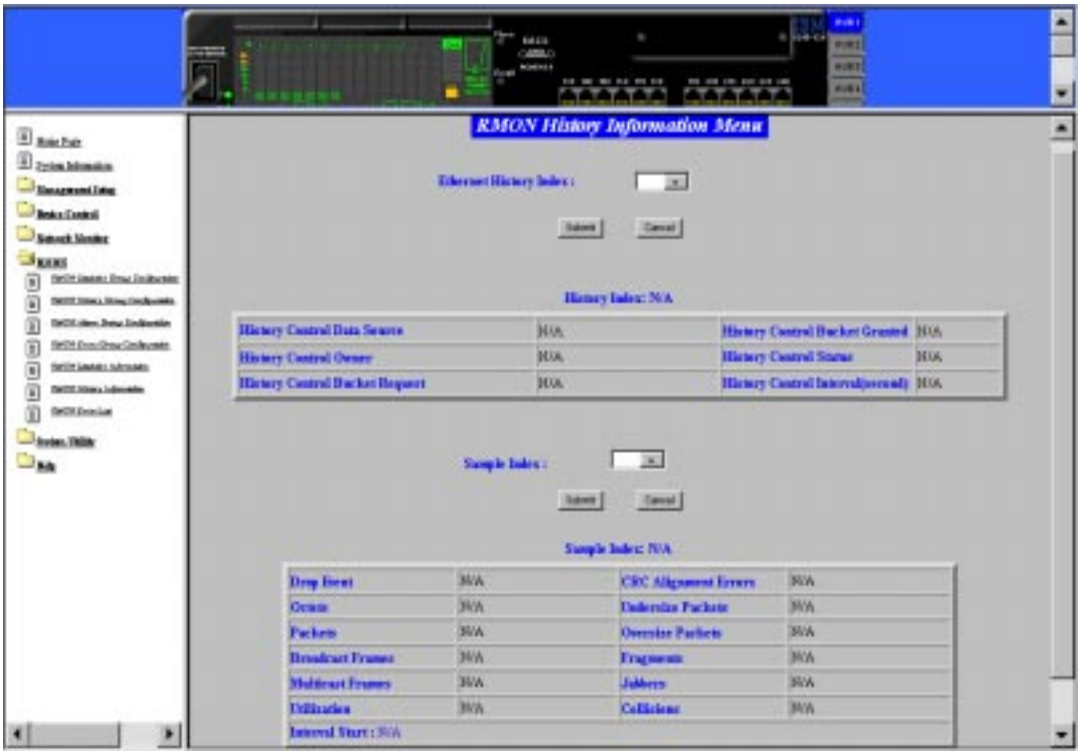


Figure 5-41 RMON History Information Menu

This menu is used to view the Ethernet information.

Ethernet History Index

The index number of a history event. The range is 1 to 65535. The maximum number of entries is 16.

History Control Data Source

10-Mbps or 100-Mbps segment.

History Control Owner

The entity that configured this entry and is using the resources assigned to it. A string of up to 12 characters is allowed.

History Control Bucket Request

Number of sample buckets you want to collect and store. The range is 1 to 65535.

History Control Bucket Granted

Number of sample buckets that will be collected and stored. The number granted is affected by available resources.

History Control Interval (seconds)

Interval in seconds, between bucket samples. The range of the interval is 1 to 3600 seconds (1 hour). The default is 1800 seconds.

History Control Status

A valid status has all fields filled in. Setting the status to invalid deletes the index. An index with incomplete information in some fields automatically sets the status as underCreation.

Valid
An entry is fully-configured and consistent.

underCreation
An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified.

Invalid
Entry is cleared.

Sample Index

The index number of the sample statistics taken based on the number of buckets granted. This index starts at 1 to a maximum of 20.

RMON Event Log

Selecting this option displays the RMON Event Log Menu as shown in Figure 5-42. You can also refer to “RMON Event Group Configuration” on page 5-77 for further information.

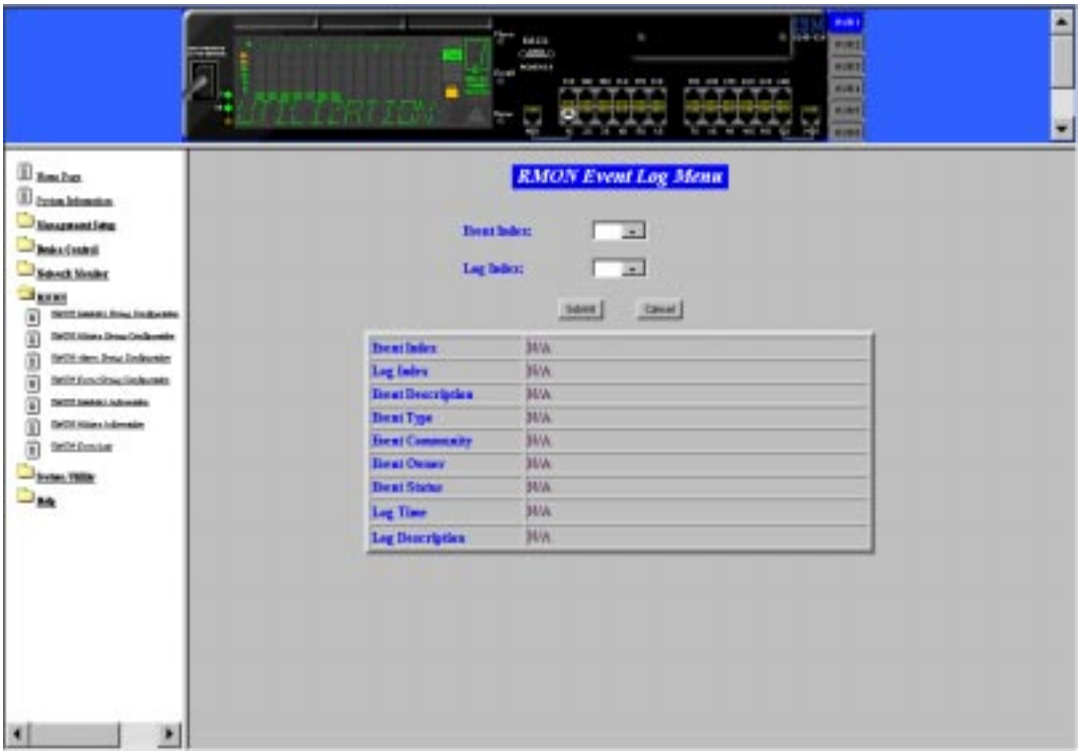


Figure 5-42 RMON Event Log Menu

This panel creates entries in an event log and sends SNMP traps to the management workstation.

Event Index

A number that identifies an entry in the event table.

Log Index

An entry is made in the log table for each event

Event Description

A comment that describes this event.

Event Type

Displays the event type.

Log

When an alarm occurs, the alarm status will be logged.

Trap

When an alarm occurs, a trap will be sent to the specified SNMP community.

Log and Trap

When an alarm occurs, the alarm status will be logged and a trap will be sent to the specified SNMP community.

Event Community

An octet string that specifies the SNMP community to which an SNMP trap is to be sent (up to 16 characters).

Event Owner

Text field to identify the owner (up to 12 characters).

Event Status

Valid

An entry is fully configured and consistent.

underCreation

An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made **underCreation** to be modified.

Invalid

Entry is cleared.

Log Time

The system time that this log was generated.

Log Description

A comment that describes this event.

System Utility

Selecting this option displays the System Restart Menu.

System Restart

Selecting this option displays the System Restart Menu as shown in Figure 5-43.

Figure 5-43 System Restart Menu

The system can be restarted using a warm start.

You can restart the system at any time without losing configuration settings, except in the case of a download. When select **SUBMIT** a warning message informs you that a system restart will be performed now.

Warm Start

A warm restart will restart the hub at the runtime code. For most cases, a warm restart is sufficient, except in the case of a BootP request or code download.

Login Timeout Interval Setup

Selecting this option displays the Login Timeout Interval Setup Menu as shown in Figure 5-44.

Figure 5-44 Login Timeout Interval Setup Menu

This panel lets you select the time after which an established Telnet session or Local Console is automatically logged out if inactive. The range is 0 to 60 minutes. The default is 5 minutes. If you specify zero, the session remains logged in regardless of how long it is inactive.

Select **SAVE** to save your changes.

Help

Selecting this option displays the Help Menu as shown in Figure 5-45, Figure 5-46 and Figure 5-47.

Figure 5-45 Help Menu-1

Content

Notice for users of Microsoft Internet Explorer

Selecting this option displays the Help Menu-2 as shown in Figure 5-46 on page 5-90. This menu gives instructions for making connections to the 10/100 Ethernet Stackable Hub 8245 using Microsoft Internet Explorer.

How to enable the trap window

Selecting this option displays the Help Menu-3 as shown in Figure 5-47 on page 5-91. This menu displays help for enabling the trap window.

Figure 5-46 displays Help for Internet Explorer users.

Figure 5-46 Help Menu-2

This menu gives instructions for making connections to the 10/100 Ethernet Stackable Hub 8245 using Microsoft Internet Explorer.

Figure 5-47 displays help for enabling the trap window.

Figure 5-47 Help Menu-3

Chapter 6. Troubleshooting and Service

This chapter contains procedures that help you troubleshoot problems with the 10/100 Ethernet Stackable Hub 8245 and its connections to other devices.

Be sure to read “Safety Information” on page xiii before proceeding.

Diagnosing Problems

The following sections contain lists of symptoms and actions to assist in problem resolution prior to contacting IBM Support.

Power-On Self-Test Failures

When the 10/100 Ethernet Stackable Hub 8245 is powered on or if a cold restart is initiated, it performs a power-on self-test (POST). If you are connected to the EIA 232 port and have your VT100-compatible terminal running, the following scrolling text appears on your monitor depending on whether the test fails or completes successfully:

```
BOOT ROM Integrity Test........ OK
BOOT ROM Integrity Test........ FAILED
       Expected checksum = 0x12345678
       Error checksum    = 0xFFFFFFFF

DRAM Test (04096 Kbytes)........ OK
DRAM Test (00000 Kbytes)........ FAILED
       Failed location = 0x80000000
       Test pattern    = 0x80001234
       Error pattern   = 0xFFFFFFFF

New Version BOOT ROM........ AVAILABLE
New Version BOOT ROM........ NOT FOUND

VFD Display Access Test........ OK
VFD Display Access Test........ FAILED

Flash Memory (512 Kbytes) Installed...... OK
Flash Memory Device Type........ UNKNOWN

Flash Memory (1024 Kbytes) Installed [2]........ OK
Flash Memory Device Type [2]........ UNKNOWN

Run Time Image Integration Test........ OK
Run Time Image Integration Test....... FAILED
-- Please reload run time image
```

```
Web-Pages Integration Test........ OK
Web-Pages Integration Test........ FAILED
-- Please reload Web-Pages

EEPROM Read/Write Test........ OK
EEPROM Read/Write Test........ FAILED

NIC Controller Access Test........ OK
NIC Controller Access Test........ FAILED

NIC Controller Loop Back Test........ OK
NIC Controller Loop Back Test........ FAILED

MAC Address = 00 4A C1 C1 23 45
Repeater Controller And Serial Management Interface Access Test...... OK
Repeater Controller And Serial Management Interface Access Test.. FAILED
```

If any of the POST fails, disconnect and reconnect the power to retry the POST.

Runtime Integrity Test Failure: If the Runtime Integrity test fails, you might have a problem that could be corrected by reloading the system software. For information on reloading your system software, see “BOOT ROM Console” on page 6-6.

Web Pages Integrity Test Failures: If the Web Pages Integrity test fails, you might have a problem that could be corrected by reloading the Web Pages Database information. For information on reloading your Web Pages Database information, see “BOOT ROM Console” on page 6-4.

If any other test fails, contact IBM Support.

Hot Plug Stack Link Cable (Software Version 1.10 and Later)

Symptom	Action
The newly added units cannot be managed after 2 minutes.	1. Check the position of the manageable and managed units to see if all the managed units are on the top of the manageable units. If not, rearrange the units as necessary. 2. Disconnect and reconnect the power to one of the units in the stack. Wait 1 minute to see if the newly added units can be managed or not. If not, go to next step. 3. Unplug the stack link cable and check if the pins are bent. 4. Follow the Instructions for “Stacking Hubs with Stack Link Cables” on page 2-10 of Chapter 2 to replace a new cable or swap it with another stack link cable in the stack. This will enable you to check if the newly added unit can be put in the stack. If not, call for service.

"Wait Data Carrier Detect" message on VFD

Symptom	Action
A "Wait DCD" message is displayed on the VFD if the following conditions occur during a restart or power on: • OOB Enabled • "Download Files" selected • TFTP server mask same as SLIP IP mask • Modem attached with no phone connection	1. Dial up modem to go into OOB downloading process. OR 2. Recycle the device power and press ENTER, while "10 sec to OOB" is being shown on the VFD, to enter BootRom Console.

Backup Managed (Software Version 1.10 and later)

Use the following instructions to fix the problem:

Symptom	Action
The active managed hub cannot duplicate the configuration of the stack to the backup managed unit.	1. Use a null-modem cable to connect to the EIA 232 port to enter into the management session. Check the software versions of the managed unit and the backup managed units to see if they are the same. If not, follow the procedures for downloading new software to ensure that all the managed units have the same level of software at version 1.10 or higher. 2. Ensure that each managed unit has a unique IP address.
You can ping the IP address of the managed unit and get its status, but you cannot get the information for hubs in the stack (the backup managed unit has powered off).	1. Check the power connection of each hub in the stack to see if one of the managed units has been powered off. 2. If not, check the stack link cable of the managed unit that connects with the first hub in the stack. Replace it if it is defective.
You cannot ping the IP address. Also, you cannot determine whether the backup managed unit has become the managed unit (the managed unit on the top of the stack has powered off).	1. Check the power connection of each hub in the stack to see if the managed unit on the top has been powered off. 2. If not, disconnect the stack link cable of the managed unit on the top of the stack to see if the backup managed unit will become the managed unit. 3. Disconnect the power of the managed unit that you had removed from the stack to see if it can function separately. If it can be booted and operated again, you can put it back into the stack. 4. If the problem cannot be fixed using the above procedures, power off each hub starting from the top of the stack and power each on again to reset the whole stack.

VFD toggles between NUM Mode and all segments lit. The Backup Managed Hub comes up with the Utilization screen displayed on the VFD and will periodically restart.	1. If you are adding a new Hub to the top of the stack, make sure that the Backup Function is enabled in the Management Capability Setup Menu of BOOT ROM Console. 2. Verify the Backup Function of the Backup Managed Hub is enabled in the Management Capability Setup Menu of the BOOT ROM Console.

BOOT ROM Console

Connect your VT100-compatible terminal emulator to the EIA 232 management port to see the POST's text messages. When the POST completes, the following message is displayed:

```
[Enter]: Abort Boot Loader
```

Notes:

1. If you do not select the abort command within 12 seconds, the hub is automatically reset.
2. The BOOT ROM menu is a subset of the functions available on the main menu of the management interface described in Chapter 4, "Using the Management Interface."

Selecting the abort command displays the BOOT ROM login panel as shown in Figure 6-1.

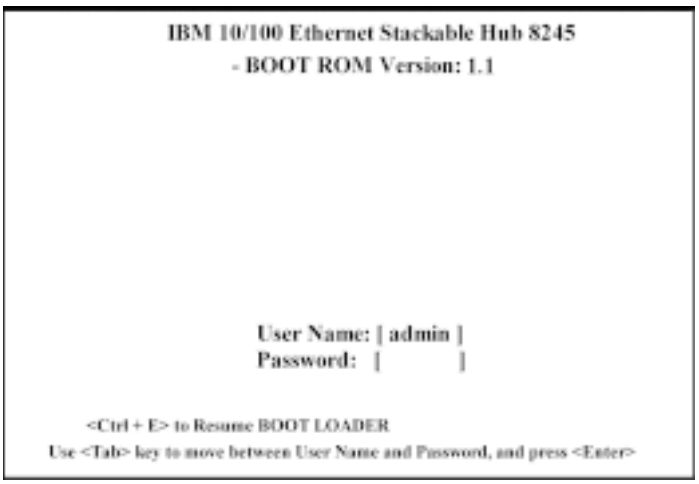


Figure 6-1 BOOT ROM Login Panel

You can log in using a previously defined user name and password, or you can use one of the default user names. One default user name, ADMIN, requires no password. The other default user name, GUEST, has a password of GUEST. (Note that user names and passwords are not case sensitive.)

After you have logged in, the BOOT ROM console main menu shown in Figure 6-2 is displayed.

Figure 6-2 BOOT ROM Main Menu

You can select **System Download** to reload the code on your 10/100 Ethernet Stackable Hub 8245. See “System Download” on page 4-61 for more information on downloading code. To exit from the main menu, select **RESUME BOOT LOAD** to continue booting the 10/100 Ethernet Stackable Hub.

Help

The Help Menu lists all the keyboard commands used in a Console session.

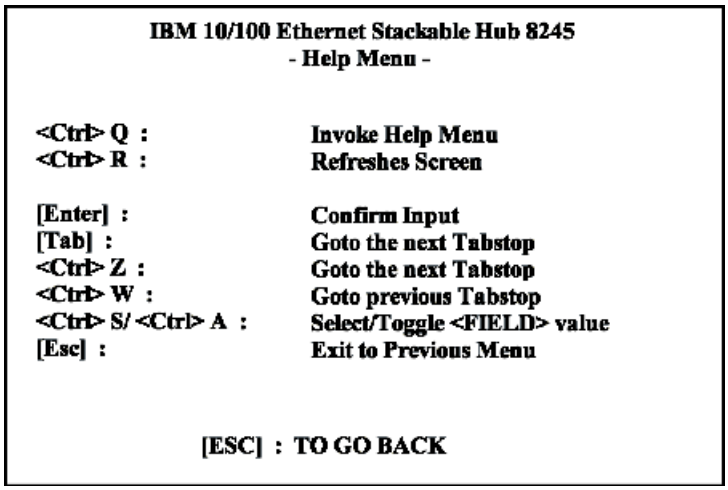


Figure 6-3 Help Menu

LEDs

Symptom	Action
Power LED does not light.	1. Check the power cable to ensure that it is firmly connected to both the hub and the power outlet. 2. Ensure that there is power at the power outlet.
OK LED is Off or fault LED is On.	The hub is malfunctioning. Repower or cold restart the hub. If the hub still fails, contact IBM Support.

Control Panel

Symptom	Action
Port Indicator and port number frame are both On.	1. The port has been disabled by changing the Admin State of the Repeater Port Control to Disable. 2. The operating status of this port is set to "Disable" by changing the Link Test State of the Repeater Port Control to Disable.
Port Number Frame is blinking.	Port has been partitioned due to a broadcast storm. Message zone displays BRDCST STORM.
Port Number Indicator On (but not bright), port number frame Off, port is available, but link is still down.	Check that: 1. All connections are secure. 2. The device at both ends of the cable are powered-on. 3. The cable is good. 4. The correct type of cable (either crossover or straight-through) is used. If connected devices are MDI-X only, ensure that you are using a crossover cable.

EIA 232 Port

Symptom	Action
Menu panels incorrectly displayed.	1. Check that the VT-100 terminal emulator is correctly configured: 9600 bps, 8 data bits, 1 stop bit, no parity, and VT-100 emulation. 2. Check that the hub is configured for console mode.

Login menu does not display.	1. Check that the VT-100 terminal emulator is correctly configured: 9600 bps, 8 data bits, 1 stop bit, no parity, and VT-100 emulation. 2. Perform the command line “wake up” procedure by pressing **Enter** two or three times or pressing **Ctrl**-**R** to refresh the panel. 3. Verify that you are using a null-modem cable or a serial cable with a null-modem adapter. 4. Check to see if OOB is displayed on the VFD.

Telnet Session

Symptom	Action
Telnet workstation cannot access the hub.	1. Check that the hub's IP address, subnet mask, and default gateway are correctly configured. 2. Ensure that you entered the IP address or host name of the hub correctly when invoking the Telnet facility. 3. Only one active Telnet session is allowed at one time.

Password

Symptom	Action
Lost control panel password.	Use the management interface (either by a Telnet session or by using the EIA 232 port) and reset the control panel password using the User Authentication Menu. (See "User Authentication" on page 4-58).
Lost control panel password (Web or Management Interface).	1. Contact network administrator for a new password. 2. Contact another user with READ/WRITE access. 3. Contact IBM Support. **Note:** If no user has READ/WRITE access, contact IBM Support.

Web Browser

Note: Web browsers must support Java 1.0 Multiframe HTML. The 10/100 Ethernet Stackable Hub 8245 has been tested using Netscape Navigator Versions 3.04, 4.03 and 4.04, and Microsoft Internet Explorer 3.02 and 4.0 in both Microsoft Windows 95 and Microsoft Windows NT 4.0.

Symptom	Action
Web browser cannot access the hub.	1. Check that the 10/100 Ethernet Stackable Hub's IP address, subnet mask and default gateway are correctly configured. 2. Ensure that you entered the IP address of the hub correctly on your Web browser. 3. If you are using Microsoft Internet Explorer, see "Help for Using Internet Explorer."
The Java applet graphic of the hub does not appear.	Clear the memory cache and the disk cache of your Web browser. For example, in Netscape 4.03 select **Edit/Preferences/Advanced/Cache** and then select **Clear Memory Cache** and **Clear Disk Cache**.

Help for Using Internet Explorer

In the Microsoft Internet Explorer, using an IP address instead of a host name can cause problems related to Java classes. You can use either of the following method to enable the Java communication in the hub panel.

Method One:

1. Construct a host entry in the host table of your local machine.

   - Place the host table file in Windows/hosts. For example, if the IP address of the hub is 212.67.1.99, and you choose a unique host name, "device 99", then you can edit the file as follows:

     - 127.0.0.1 localhost

     - 212.67.1.99 device99

2. Type **device99** in the URL text field of IE 3.0 or IE 4.0 to get the HTML document and download the Java class.

Method Two: Create the host entry in the host table of one Domain Name Server and setup the domain name server of your local machine.

Note: Method One is the recommended method.

When managing the 10/100 Ethernet Stackable Hub Model 112 and 124 with default settings of Microsoft Internet Explorer 4.0 (IE4), the Java Applet fails to display the picture of the hub. This occurs with IE4 running on Windows 95, Windows 98, or Windows NT.

To enable your browser to work correctly with the 10/100 Ethernet Stackable Hub Model 112 and 124, it will be necessary to make the following changes:

Step 1. Select the browser's **View** pull-down menu and select Internet Options.

Step 2. Select the **Advanced** tab and locate the Java VM heading.

Step 3. Under Java VM select **Java console enabled** and then Apply.

Step 4. Select the **Security** tab and then the **Custom** radio button.

Step 5. Select **Setting** and locate the **Java** menu heading.

Step 6. Under **Java permissions** select **Custom**.

Step 7. Select **Java Custom Setting**.

Step 8. Select the **Edit Permissions** tab.

Step 9. Under the unsigned Content, locate the Run Unsigned Content section and select **Enable**.

Step 10. Select **OK** - **OK** - **Apply** - **OK**.

Step 11. Exit and re-enter your web browser.

If your browser does not have this content, you may have to download IEAK (Internet Explorer Administration Kit).

The software can be downloaded through http://ieak.microsoft.com.

Obtaining Software

You can obtain the latest level of code, MIBs, tips, and publications about the 10/100 Ethernet Stackable Hub 8245 through the Internet.

WWW Site

1. Access the IBM Networking Technical Support:

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

2. Select 8245 for the Product Number menu.

   You can access product announcements, publications, technical tips, and code downloads. You can also subscribe to receive e-mail notifications of code updates, tips, and FAQs for the 10/100 Ethernet Stackable Hub 8245.

3. Locate and download the following file 8245Vxxx.EXE. The file includes BOOT ROM, Web pages database information, system software code, and readme file.

   Note: In this filename, xxx is the version number.

Obtaining Service

If you need assistance in troubleshooting or if you need service for your 10/100 Ethernet Stackable Hub 8245, call IBM at **1 800 772-2227** in the United States and **1 800 426-7378 (1 800 IBM-SERV)** in Canada. See Appendix A, "Notices," for information concerning service for the product.

Appendix A. 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 in this publication 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, programs, or services, 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, North Castle Drive, Armonk, NY 10504-1785, USA.

Notice to Users of Online Versions of This Book

For online versions of this book, we authorize you to:

Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.

Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine-readable documentation.

Safety Notices

Telecommunications Safety Requirements in the United Kingdom

This IBM product is made to high safety standards. It complies inherently with telecommunications safety standard BS 6301. It is not designed to provide protection from excessive voltages appearing externally at its interfaces. Therefore, when this product is connected to a public telecommunications network via any other equipment, and you connect to this product items not supplied by IBM United Kingdom Ltd., you must comply with mandatory telecommunications safety requirements.

Statement of Compliance with the United Kingdom Telecommunications Act 1984

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connections to the public telecommunications systems in the United Kingdom.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

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 NMB-003 du Canada.

European Norm (EN) 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 an 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 typical residential environments to provide reasonable protection against interference with licensed communication devices.

Warning: 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:

Das Gerät erfüllt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich funkstorungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßbnahmen durchzufuhren und dafur 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 verößern."

Anmerkung
Um die Einhaltung des EMVG sicherzusellen 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。

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。

Trademarks

IBM is a trademark of the IBM Corporation in the United States or other countries or both.

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 other companies.

International Business Machines Corporation *Armonk, NY 10504*

Statement of Limited Warranty

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

Machine	8245 10/100 Ethernet Stackable Hub Models 012, 024, 112 and 124
Warranty Period*	One Year

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

Production Status

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

The IBM Warranty

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

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

For a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade.

Some of these transactions (called "Net-Priced" transactions) may include additional parts and associated replacement parts that are provided on an exchange basis. All removed parts become the property of IBM and must be returned to IBM.

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

If a Machine does not function as warranted during the warranty period, IBM in its sole discretion will repair, replace it (with a Machine that is at least functionally equivalent), or refund the purchase price. To obtain coverage under the warranty you may be required to present proof of purchase.This warranty is non-transferable by the end-user customer.

This warranty is non-transferable by the end-user customer.

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.

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

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

It is your responsibility to:

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

Extent of Warranty

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

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

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

In Canada, warranties include both warranties and conditions.

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

Limitation of Liability

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

1. bodily injury (including death), and damage to real property and tangible personal property; and
2. the amount of any other actual loss or damage, up to the greater of $100,000 or the charge for the Machine that is the subject of the claim.

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

1. third-party claims against you for losses or damages (other than those under the first item listed above);
2. loss of, or damage to, your records or data; or
3. economic consequential damages (including lost profits or savings) or incidental damages, even if IBM is informed of their possibility.

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

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

Appendix B. Cable Pinout Diagrams

Straight-Through 10BASE-T/100BASE-TX Cables

10BASE-T/100BASE-TX connections to devices such as workstations and servers require straight-through cables, as shown in Figure B-1 and B-2 for UTP cable and Figure B-3 on page B-2 for STP cable.

Two standards are shown for wiring UTP connectors, T568-A and T568-B. The only difference between them is in the color of the insulation around the wires.

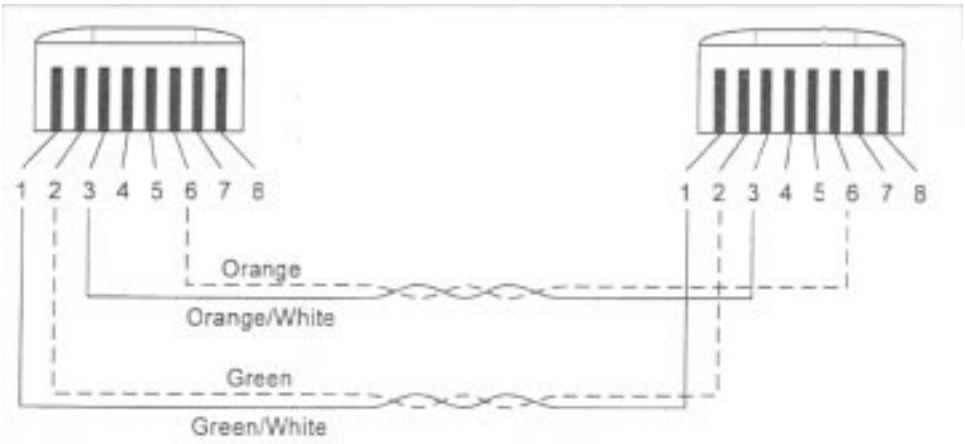


Figure B-1. Straight-Through UTP Cable (RJ-45 to RJ-45), T568A

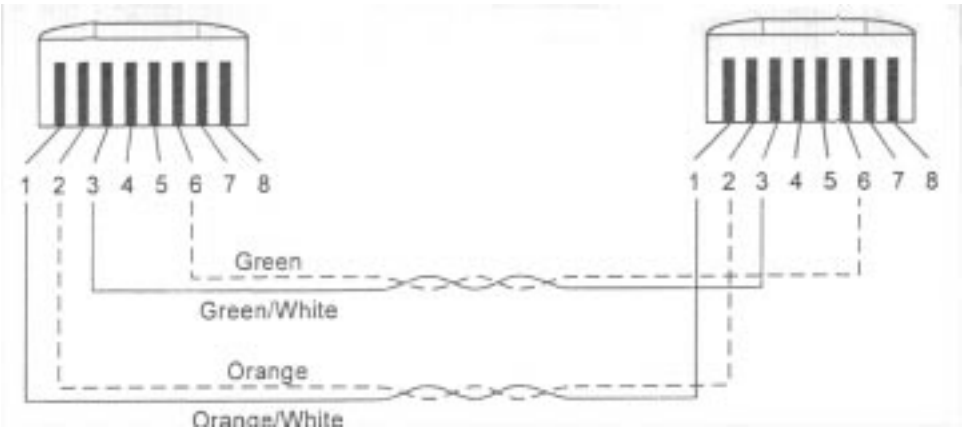


Figure B-2. Straight-Through UTP Cable (RJ-45 to RJ-45), T568B

Straight-Through 10BASE-T/100BASE-TX Cables for STP

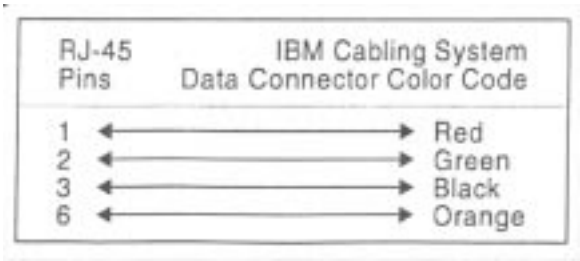


Figure B-3. Straight-Through STP Cable (RJ-45 to IBM Data Connector)

Crossover 10BASE-T/100BASE-TX Cables

Crossover cables are typically required when making 10BASE-T/100BASE-TX connections to other hubs. The 8245 does not require crossover cables, but if you need them, Figure B-4 and Figure B-5 on page B-3 show you how to wire the connectors for UTP cabling and Figure B-6 on page B-3 shows you how to wire the connectors for STP cabling.

Two standards are shown for wiring UTP connectors, T568-A and T568-B. The only difference between them is in the color of the insulation around the wires.

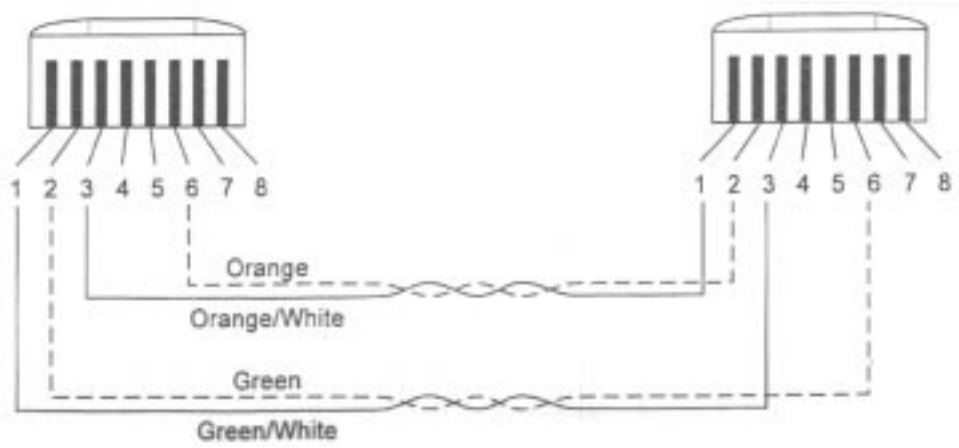


Figure B-4. Crossover UTP Cable (RJ-45 to RJ-45), T568-A

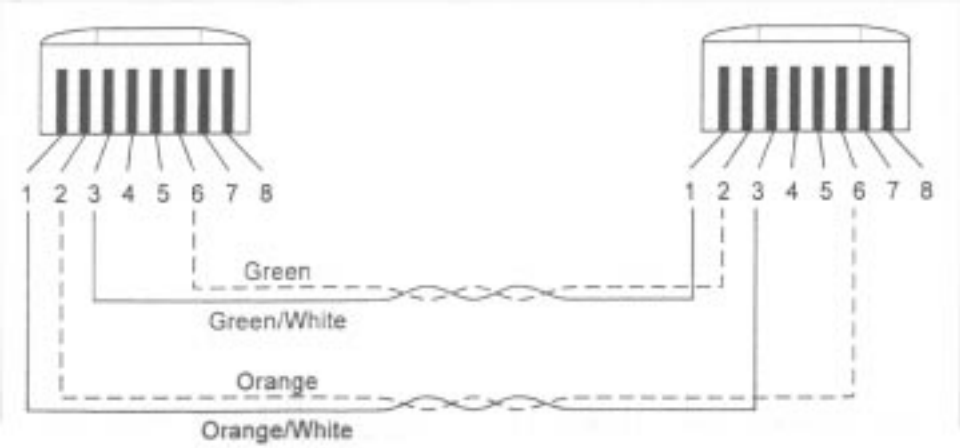


Figure B-5. Crossover UTP Cable (RJ-45 to RJ-45), T568-B

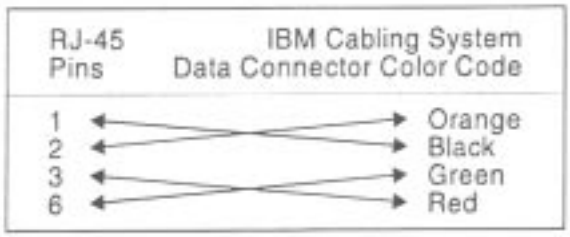


Figure B-6. Crossover STP Cable (RJ-45 to IBM Data Connector)

Null-Modem Cable

A null-modem cable should be used for a direct connection from a PC serial port to the 8245 Management Port.

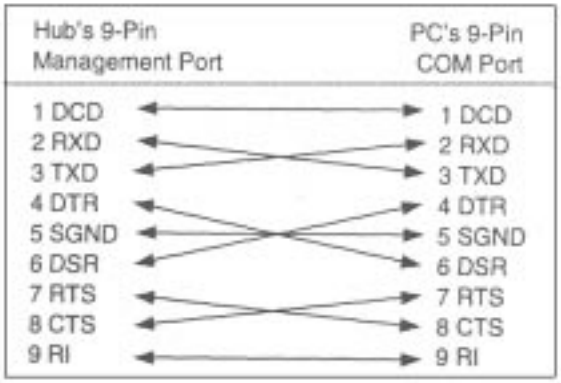


Figure B-7. Null Modem Cable Connection

Index

Tell Us What You Think?

IBM 10/100 Ethernet Stackable Hub 8245
Installation and Planning Guide
Part Number 31L3912

We hope you find this publication useful, readable, and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form. If you are in the U.S.A., you can mail this form postage free or fax it to us at 1-800-253-3520. Elsewhere, your local IBM branch office or representative will forward your comments or you may mail them directly to us.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or problems

Please tell us how we can improve this book:

Thanks you for your comments. If you would like a reply, provide the necessary information below.

Name

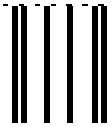
Address

Company or Organization

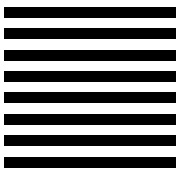
Phone Number

Tell Us What You Think!
31L3912

Cut or Fold
Along Line



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAILPERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Design & Information Development
Dept. CGF/Bldg. 656
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape Please do not staple Fold and Tape

31L3912

Cut or Fold
Along Line

Part Number: 31L3912

Printed in Taiwan

Web sites:

8245 Product Support
www.networking.ibm.com/support/8245

Networking Product Sales
www.networking.ibm.com

Networking Product Support
www.networking.ibm.com/support