FHU-1201/1202/2401/2402TFXS

Stackable Ethernet Hubs

User's Manual

DOC No.: GB0110M801

FCC Warning

This device has been tested and found to comply with 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 user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

CE Mark 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.

Table of Contents

CHAPTER 1 INTRODUCTION 1-1

About Dual Speed Hub FHU-1201/1202/2401/2402TFXS 1-1
Dual Speed Hub FHU-1201/1202TFXS 1-1
Dual Speed Hub FHU-2401/2402TFXS 1-2
Key Features 1-3
10/100Mbps Auto Sensing Ports 1-3
Stackability 1-3
Expansion Slots 1-4
Manageability 1-4
RMON Probe Capability 1-4
Offline Operation 1-5
Proactive Monitoring 1-5
Problem Detection and Reporting 1-5
Value Added Data 1-5
Multiple Managers 1-5
Redundant Link Capacity 1-5
Address Tracking Capability 1-6
Source Address Search Capability 1-6
Security Intrusion Control Capability 1-6
Broadcast Storm Detection and Protection Capability 1-7
Hub FHU-1201/2401TFXS Front Panel Overview 1-7
LED Indication 1-8
Power 1-8
Link/Rx 1-9
Collision 1-9
Forward 1-9
Internal Switch (Bridge) 1-10
External Switch (Bridge) 1-10
Hub ID 1-10
Hub FHU-1202/2402TFXS Front Panel Overview 1-11
Mini-Console 1-11
Rear Panel Layout 1-12

CHAPTER 2 INSTALLATION 2-1

Hub Location 2-1
Stacking Hub FHU-1201/1202/2401/2402TFXS Series 2-1
Rack Mounting 2-2

Stacking Hubs using Daisy Chain Cables 2-3
Constructing a Management Hub Stack 2-4
Position within the Stack 2-4
Master Hub Role 2-4
Slave Hub Role 2-5
Hub ID/Position within the Stack 2-5
Segmenting Hubs 2-5
Connecting Other Network Devices 2-5
Connecting Cables 2-5
Connecting Workstations 2-6
Connecting Ethernet Hubs or Devices 2-7
Connecting Fast Ethernet Switching Hubs 2-8
Connecting the Other Dual Speed Hubs 2-9

CHAPTER 3 USING EXPANSION MODULES 3-1

Expansion Module Overview 3-1
Internal Bridge Function 3-1
External Bridge Function 3-2
Backpressure (flow control) 3-2
Installing a Bridge Module 3-2
TX Module LED Indicators 3-4
TF Module LED Indicators 3-5
Module MDU-0112TX 3-6
ModuleMDU-0112TX Jumpers 3-6
Module MDU-0112TX Backpressure Jumpers 3-7
Module MDU-0205TX 3-7
Module MDU-0205TX Jumpers 3-8
Module MDU-0205TX Backpressure Jumpers 3-8
Module MDU-0113FX 3-9
Module MDU-0113FX Jumpers 3-9
Module MDU-0113FX Backpressure Jumpers 3-10
Module MDU-0206FX 3-10
Module MDU-0206FX Backpressure Jumpers 3-11

CHAPTER 4 MANAGING HUB THROUGH MINI-CONSOLE 4-1

Mini-Console Overview 4-1
Features 4-1
Mini-Console Display Panel 4-2
VFD Display 4-3
% The relative percentage of utilization or collision. 4-3

Port Number Indicators (1 to 12)....4-3
Port Indicator Frame ( )....4-3
Message Zone....4-3
Gauge Bars....4-3
Lock Icon Indicates the control panel configuration is locked....4-3
G-A Port group indicator displays status of ports 1 to 12....4-3
G-B Ports 13 to 24....4-3
Master Indicates this hub is a master hub....4-3
SNMP Indicates the hub is SNMP manageable....4-3
WWW Indicates the Web Management feature is enabled....4-3
OOB Indicates that out-of-band is enabled....4-3
Observing Basic Port Information....4-4
Port Indicator Definition....4-4
Console Keys....4-4
Menu Tree....4-5
Observing Network Traffic....4-8
Selecting Group....4-9
Monitoring Port Statistics....4-10
Selecting a port to monitor....4-11
Monitoring Port Detail Information....4-13
Monitoring All Ports Status....4-13
Monitoring Individual Port Status....4-15
Configuring Ports....4-16
Configuring ALL PORTS:....4-17
Configuring a single port....4-18
Unit Configuration....4-19
Configuring the unit....4-19
Lock the Mini-Console....4-20
Unlock the Mini-Console....4-21
Network Configuration....4-22
IP Address Configuration....4-22
Subnet Mask....4-24
Default Gateway....4-24
Out-of-Band Configuration....4-24
Securing the Hub....4-24
Set Password....4-25
Cancel Password....4-25
In Case You Forget Your Password....4-26
Restart the Hub....4-26
Restore System Default Settings....4-26
About the Hub....4-27
System Information....4-27

CHAPTER 5 CONSOLE MANAGEMENT.....5-1

Connecting the Console Interface 5-2
Menu Convention 5-3
Menu Title.....5-4
Check Box.....5-4
Toggle Input Item.....5-4
Text Item Item.....5-4
Item Selected.....5-5
Commands 5-5
Message Line 5-5
Using the Console Program..... 5-5
Logging In 5-6
Main Menu 5-7
System Information.....5-7
Management Setup.....5-7
Device Control 5-8
Network Monitor.....5-8
User Authentication 5-8
System Utility.....5-8
Monitoring System Information 5-8
System Description.....5-9
System Object ID.....5-9
System Up Time.....5-9
System Contact 5-9
System Name 5-9
System Location.....5-9
Setting up for Management 5-10
Network Configuration 5-10
Serial Port Configuration 5-10
SNMP Community Setup.....5-10
Trap Receiver.....5-10
Management Capability Setup.....5-11
Trap Filter 5-11
Network Configuration.....5-11
Local Console/Remote Telnet-Ethernet.....5-11
Local Console/Remote Telnet-SLIP 5-13
Serial Port Configuration.....5-15
Console Mode.....5-15
Out-Of-Band Mode.....5-15
SNMP Community Setup 5-17
To add a community name:.....5-18
To edit a community name: 5-18

Trap Receiver Setup 5-18
Web-Based Management Configuration 5-21
Trap Filter 5-22
Controlling Devices 5-23
Repeater Group Control/Status 5-24
Repeater Port Control/Status 5-24
2/3-Port Bridge Module Control/Status 5-24
External AUI Module Control/Status 5-24
Redundant Link Control 5-24
Security Intrusion 5-24
Repeater Group Control/Status 5-25
Group Status 5-25
Group Control 5-26
To change the setting of a given group: 5-28
Repeater Port Control/Status 5-29
Port Status 5-29
Port Control 5-31
2/3-Port Bridge Module Control/Status 5-32
Bridge Module Status 5-32
Bridge Module Control 5-33
Redundant Link Control 5-35
Configuring Link Pairs 5-38
Editing a Link Pair 5-39
Deleting a Link Pair 5-39
Security Intrusion 5-39
Monitoring Network 5-42
Repeater Statistics Information 5-43
Repeater Group Statistics Information 5-45
Absolute 5-45
Relative 5-46
Repeater Port Statistics Information 5-47
Absolute 5-47
Relative 5-48
Address Tracking Information 5-51
Address Search Information 5-53
Broadcast Storm Protection 5-55
Formula for calculating Broadcast packet rate 5-57
Broadcast Storm Detected 5-57
User Authentication 5-58
System Utility 5-60
System Download 5-61
To download TFTP code, perform the following: 5-62
System Restart 5-63

Factory Reset 5-64
To perform the factory reset, do the following steps:.....5-64
Login Timeout Interval 5-65
Configuration Upload Setting 5-66
Configuration Upload Request.....5-67

CHAPTER 6 SNMP MANAGEMENT.....6-1

Managing via MIB File..... 6-1
Managing through HP-OpenView..... 6-1

APPENDIX A PRODUCT SPECIFICATIONS A-1

APPENDIX B ERROR MESSAGES.....B-1

APPENDIX CMINI-CONSOLE MENU TRE E.....C-1

APPENDIX D TROUBLESHOOTING.....D-1

APPENDIX E INDEX..... E-1

Chapter 1

Introduction

About Dual Speed Hub FHU-1201/1202/2401/2402TFXS

Dual speed FHU-1201/1202/2401/2402TFXS is a family of auto sensing dual speed, manageable and stackable hubs. The Hub FHU-1201/1202/2401/ /2402TFXS Family consists of masters, up-gradeable masters and managed slaves with 12 or 24 ports. The features and functions of the Hub FHU-1201/1202/2401/2402TFXS family make it a powerful, cost effective solution for large campus networks, schools and rapid growth companies.

All models in the Hub FHU-1201/1202/2401/2402TFXS family accept slide-in expansion modules, adding more power and versatility, such as: *Bridging 10 Mbps and 100 Mbps segments*, and *extending distances* up to 2 kilometers.

Dual Speed Hub FHU-1201/1202TFXS

The twelve port models are FHU-1202TFXS master, and FHU-1201TFXS managed slave.

The FHU-1202TFXS master model shown in Figure 1.1 includes a Network Management Unit (NMU), Mini-Console, 12-dual-speed auto sensing ports, 2-MDI ports and a switch module expansion slot.

Figure 1.1 Dual Speed Hub FHU-1202TFXS (Master with NMU)

The FHU-1201TFXS managed slave model shown in Figure 1.2, includes an LED panel, 12-dual-speed auto sensing ports, 2-MDI ports, a switch module expansion slot. The FHU-1201TFXS can be fully managed by any FHU-1202/2402TFXS model.

Figure 1.2 Dual Speed Hub FHU-1201TFXS (Managed Slave)

Dual Speed Hub FHU-2401/2402TFXS

The twenty-four port models are FHU-2402TFXS (master) and FHU-2401TFXS (slave).

The FHU-2402TFXS master model shown in Figure 1.3 includes a Network Management Unit (NMU), Mini-Console, 24-dual-speed auto sensing ports, 2-MDI ports and a switch module expansion slot.

Figure 1.3 Dual Speed Hub FHU-2402TFXS (Master with NMU)

The FHU-2401TFXS Managed Slave model shown in Figure 1.4, includes an LED panel, 24-dual-speed auto sensing ports, 2-MDI ports, a switch module expansion slot. The FHU-2401TFXS can be fully managed by any FHU-1202/2402TFXS model.

Figure 1.4 Dual Speed Hub FHU-2401TFXS (Managed Slave)

Key Features

Dual Speed Hub FHU-1201/1202/2401/2402TFXS has many advanced features:

10/100Mbps Auto Sensing Ports

All ports, in the Dual Speed Hub FHU-1201/1202/2401/2402TFXS family are, dual speed auto sensing ports, including the MDI-II ports. Hubs automatically detect the transmission speed and set the port accordingly.

Stackability

Every model in the Dual Speed Hub FHU-1201/1202/2401/2402TFXS family is compatible, and can be configured in the same stack of up to 6 hubs in total, using daisy chain cables.

Expansion Slots

Every model in the Dual Speed Hub FHU-1201/1202/2401/2402TFXS family has two expansion slots for adding expansion modules, see Figure 1.5. The upper expansion slot is for Network Management Unit (NMU) modules only, and the lower slot accepts switch expansion modules. See Chapter 3, “Using Expansion Modules” for more information.

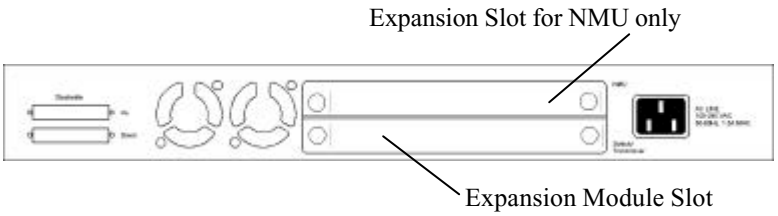


Figure 1.5 Expansion Slots

Manageability

The Hub FHU-1201/1202/2401/2402TFXS family provides extensive management capabilities including: Mini-Console Management for device level management, Console Management using a VT-100 terminal emulator, Web Management using a Web Browser or SNMP network management.

- **Mini-Console Management**
- **Local Console/Remote Telnet**
- **Out-of-Band Management**
- **Web-Based Management**
- **SNMP Management**

RMON Probe Capability

Remote network monitoring (RMON) probe is an instrument that exists for the purpose of managing a network. The goals of RMON probe are described in the following sections; Offline Operation, Proactive Monitoring, Problem

detection and Reporting, Value Added Data, and multiple managers. The Hub FHU-1201/1202/2401/2402TFXS family supports RMON group (1) statistics, group (2) History, group (3) Alarm, and group (9) Event.

Offline Operation

This MIB allows a probe to be configured to perform diagnostics and to collect statistics continuously, even when communications with the management station may not be possible or efficient.

Proactive Monitoring

The monitor can notify the management station of failure and can store historical statistical information about the failure. The management station can play this historical information back in an attempt to perform further diagnosis into the cause of the problem.

Problem Detection and Reporting

The monitor can be configured to recognize conditions, most notably error conditions, and continuously to check for them. When one of these conditions occurs, the event may be logged, and management stations may be notified in a number of ways.

Value Added Data

By highlighting those hosts on the network that generate the most traffic or errors, the probe can give the management station precisely the information it needs to solve a class of problems.

Multiple Managers

Remote monitoring can deal with multiple management stations using its resources concurrently.

Redundant Link Capacity

Redundant links can be configured enabling up to 24 pairs in a Hub FHU-1201/1202/2401/2402TFXS stack. For each pair of redundant links one port must be set as the primary and active, the other as back up and isolated. If the

primary port fails, it is isolated and set as the backup, and the backup port is set to primary and active.

Address Tracking Capability

Hub FHU-1201/1202/2401/2402TFXS provides MAC Address based tracking capability for traffic analysis to diagnose network problems such as Intrusion. This function records the source MAC address of each data packet received by the port and provides the filter for data analysis. Up to 15 source MAC addresses can be detected on each port.

Source Address Search Capability

Hub FHU-1201/1202/2401/2402TFXS provides Source Address Search Capability. This active address tracking capability is used to watch for a given MAC address and report which port is was seen on. This capability can be used to collect the necessary information for mapping the topology of a network. Up to 8 MAC addresses can be searched simultaneously. You can configure address search parameters, including Address Search Lock, Source MAC address to be searched, Address Search Status and address Search Owner with local console management, Web-Based Management or SNMP management.

Security Intrusion Control Capability

Hub FHU-1201/1202/2401/2402TFXS provides MAC Address based Security Intrusion Control Capability to prevent any unauthorized node to access the network. You can configure the hub to take various actions when a violation is detected. Actions include, no action, sending a trap message or partitioning a port.

Broadcast Storm Detection and Protection Capability

Hub FHU-1201/1202/2401/2402TFXS provides Broadcast Storm Detection and Protection Capability by periodically monitoring the broadcast counters of each port to detect broadcast storm. Ports detected causing broadcast storm are automatically partitioned, a trap is set to the network manager, or no action is taken, depending on the configuration.

Hub FHU-1201/2401TFXS Front Panel Overview

An LED panel, 12 dual speed, auto-sensing ports, switch module installed LED, and 2 MDI-II shared ports are supported on the front panel of Hub FHU-1201TFXS. See Figure 1.6.

The switch module installed LED is on if a switch module is installed in the hub.

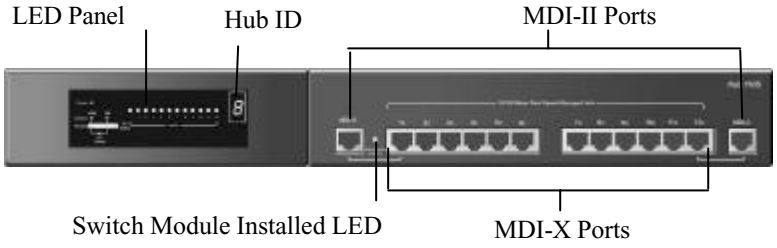


Figure 1.6 Front Panel FHU-1201TFXS (12 Ports)

An LED panel, 24 dual speed, auto-sensing ports, switch module installed LED, and 2 MDI-II shared ports are supported on the front panel of Hub FHU-2401TFXS. See Figure 1.7.

The switch module installed LED is *on*, if a switch module is installed in the hub.

Figure 1.7 Front Panel FHU-2401TFXS (24 Ports)

LED Indication

Hub FHU-1201/2401TFXS's LEDs indicate status information for the device, its ports for both segments (10Mbps and 100 Mbps), and switch status.

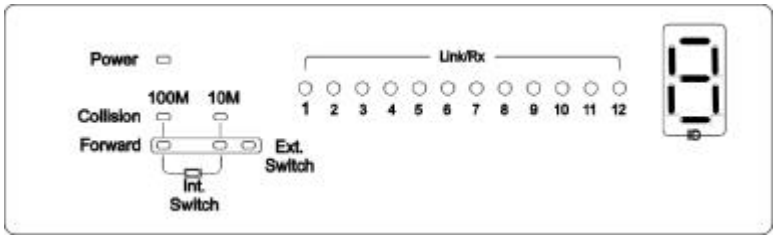


Figure 1.8 LED Indicators 12 Port

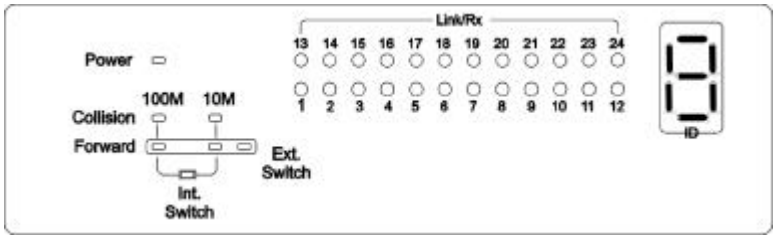


Figure 1.9 LED Indicators 12 Port

Power

The Power LED is on when the power cable is plugged into the hub and a wall socket.

Link/Rx

The Link/Rx LED is on for each connected port and blink for ports receiving transmissions.

Collision

Collision LEDs indicate collision for either segment (10 Mbps and 100 Mbps). If there is collision in a segment the LED for that segment is on.

Forward

Packet forwarding is active via switch module to connect both 10 Mbps and 100 Mbps domains. Forward LED indicates the packet forward status through switch modules. Forward for both segments (10 Mbps and 100 Mbps) are indicated below.

Forwarding LED indicator meaning

Forward LED	Status	Int Switch	Ext Switch	Meaning
100M LED	On	On	Off	A 10Mbps transmission being received by a 100 Mbps segment through the *internal switch*
100M LED	On	Off	On	A 10Mbps transmission being received by a 100 Mbps segment through the *external switch*
10M LED	On	On	Off	A 100 Mbps transmission being received by 10 Mbps segment through the *internal switch*
10M LED	On	Off	On	A 100 Mbps transmission being received by 10 Mbps segment through the *external switch*

100M LED	On	On	On	A 10 Mbps transmission being received by 100 Mbps segment through the *internal switch and through the external distance extender (Module MDU-0205TX and MDU-0206FX only)*
10M LED	On	On	On	A 100 Mbps transmission being received by 10 Mbps segment through the *internal switch and through the external distance extender (Module MDU-0205TX and MDU-0206FX only)*

Internal Switch (Bridge)

The Internal Switch LED is always *on* when the internal switch (bridge) function is active and forwarding the data.

External Switch (Bridge)

The External Switch LED is *on* when data is being forwarded from one segment to the other segment through the external switch port.

Hub ID

Each linked hub is automatically assigned a hub ID number and this number is indicated in the ID indicator. See Figure 1.6.

Hub FHU-1202/2402TFXS Front Panel Overview

The front panel for model FHU-1202TFXS supports the Mini-Console, switch module installed LED, 12-10/100 ports, and 2-MDI-II ports. The switch module installed LED is on if a switch module is installed.

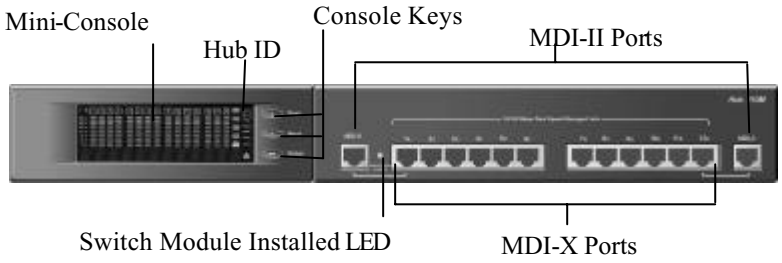


Figure 1.10 Front Panel Hub FHU-1202TFXS (12 Port)

The front panel for model FHU-2402TFXS supports the Mini-Console, switch module installed LED, 24-10/100 ports, and 2-MDI-II ports. The switch module installed LED is on if a switch module is installed.

Figure 1.11 Front Panel Hub FHU-2402TFXS (24 Port)

Mini-Console

The Mini-Console is a high definition display and Console keys that enable you to easily monitor and configure the system. The Mini-Console provides watch diagnostic functions, including port settings, status monitoring, traffic utilization, collision, and error rate.

With the Mini-Console, You can configure each device in a Hub FHU-1201/1202/2401/2402TFXS stack and all of their ports. For more information see Chapter 4 “Managing through the Mini-Console”.

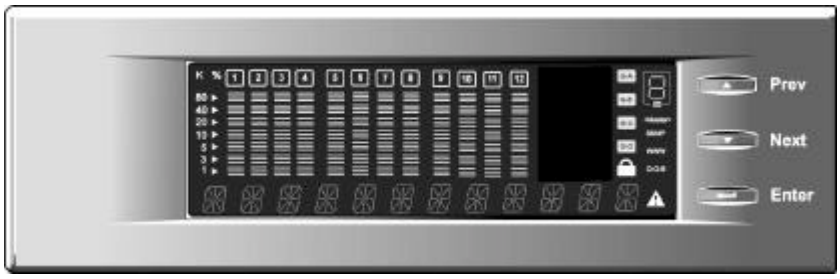


Figure 1.12 Mini-Console

Rear Panel Layout

The rear panel of each hub in the Hub FHU-1201/1202/2401/2402TFXS family supports 2-expansion slots, two- daisy-chain ports and an AC power socket.

The daisy-chain ports are used for cascading hubs (stacking hubs); the Up port of one hub must be connected to the Down port of the other hub.

The upper expansion slot accepts only NMU modules and the lower expansion slot accepts expansion modules. For information about expansion modules see Chapter 3 “Using Expansion Modules”.

The AC power socket can be safely plugged into 100~240 VAC outlets.

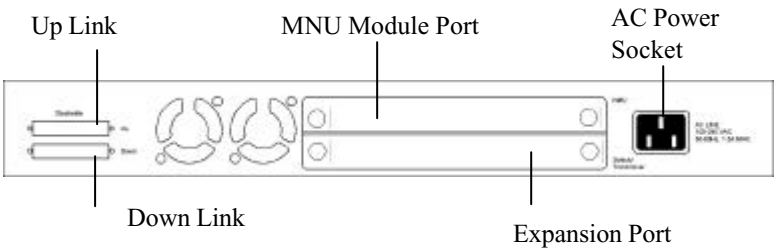


Figure 1.13 Rear Panel Layout

Chapter 2

Installation

Hub Location

Hub FHU-1201/1202/2401/2402TFXS's location should be less than 100 meters from servers, workstations, or switches. The Hub FHU-1201/1202/ 2401/2402TFXS can be desk mounted or rack mounted.

Caution: Category 5 UTP/STP cables are environment-sensitive, make sure that the cable route is not too close to electrical noise sources such as power lines or fluorescent lights.

Stacking Hub FHU-1201/1202/ 2401/2402TFXS Series

The Hub FHU-1201/1202/2401/2402TFXS series is stackable in standard 19" racks. Up to six hubs can be stacked with daisy chain cables. One master and up to five slaves can make up a stack. The master can be positioned anywhere in the stack, so you can add to a stack without re-positioning the hubs.

Rack Mounting

Optional rack mounting brackets are available to mount hubs in standard EIA 19-inch racks.

Align the mounting brackets on the sides of the unit with the slit over the holes. Secure the screws tightly to fix the brackets to the device. Then, place the device into the 19" rack and fix it properly. Please ensure that the ventilation holes do not get blocked.

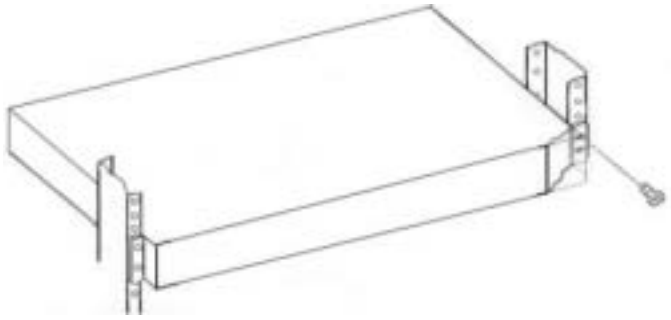


Figure 2.1 Rack Mounting

Stacking Hubs using Daisy Chain Cables

You can stack the Hub FHU-1201/1202/2401/2402TFXS family hubs using daisy chain cables. The master hub can be placed anywhere in the stack. By cascading the hub stack, each hub can be identified and assigned an ID number according to its position in the stack.

Cascading hubs with daisy chain cables to make a stack is as simple as connecting the Up Port of one hub to the Down Port of another hub illustrated in Figure 2.2.

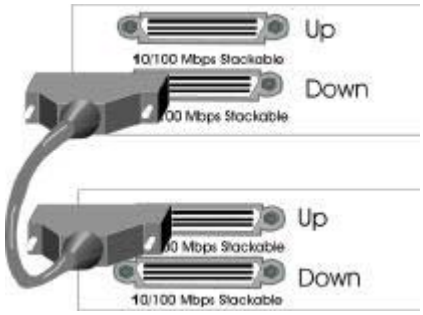


Figure 2.2 Daisy Chain Ports

Caution: To connect daisy chain cable, the Up port on one hub should connect to the Down port of another hub.

Constructing a Management Hub Stack

A stack can be constructed with up to six hubs in total. One master hub and up to five slave hubs can exist in the stack.

Position within the Stack

The master hub can be positioned anywhere in a Hub FHU-1201/1202/ 2401/2402TFXS stack and automatically assigns the hub ID of each hub according to its position in the stack.

Master Hub Role

The master is used to manage and configure other hubs in the stack and supplies the stack with additional ports (12/24) and an additional expansion module slot. The master hub can also be used as a stand-alone intelligent hub. Managing the hubs can be accomplished with the master hub's versatile management capabilities, such as;

Mini-Console Management
Described in Chapter 4 "Managing Hub through Mini-Console"

Console Management
Described in Chapter 5 "Console Management for Hub FHU-1202/ 2402TFXS"

Web Based Management
Described in "Hub FHU-1202/2402TFXS Network Management Manual"

SNMP Management
Described in "Hub FHU-1202/2402TFXS Network Management Manual"

Slave Hub Role

Slave hubs supply the stack with additional ports (12/24) and an additional expansion module slot. Slave hubs can be positioned above or below the master hub. The Hub FHU-1201/2401TFXS can also act as a stand alone dumb hub.

Hub ID/Position within the Stack

The master hub and slave hubs can be positioned anywhere in the stack and each hub's ID is automatically assigned based on its position (in the stack).

Segmenting Hubs

Hub FHU-1201/1202/2401/2402TFXS hubs can isolate one or both segments (10 Mbps and 100 Mbps segments) from the other hubs in a stack. When a segment is segmented it will not repeat to the other segment in the hub nor to segments in other hubs. For more information see "Group Admin State" on page 5-26.

Connecting Other Network Devices

Dual speed Hub FHU-1201/1202/2401/2402TFXS can connect to 10 Mbps, 100 Mbps, or 10/100 Mbps devices due to its auto-sensing capability. Hub FHU-1201/1202/2401/2402TFXS will auto-sense the connected port speed set its port to match the speed of the connected port.

Connecting Cables

Hub FHU-1201/1202/2401/2402TFXS' ports, accept Cat 3, 4 and 5 cables with RJ-45 connectors for 10 Mbps connections and Cat 5 cables with RJ-45

connectors for 100 Mbps connections. The maximum length of cables, between hub and workstations is 100 meters. The maximum length of cables, between hub and hub is 5 meters for 100 Mbps connections and 100 meters for 10 Mbps connections. All ports are hot pluggable. It is recommended to label each cable to identify the device or port at each end.

Connecting Workstations

Install either 10BASE-T or 100BASE-TX Fast Ethernet Network Interface Card into each workstation if not already installed**.** Using a UTP/STP cable, connect the Ethernet card (in the workstation) to a Hub FHU-1201/1202/ 2401/2402TFXS port as shown in Figure 2.3.

Figure 2.3 Connecting Workstations

Connecting Ethernet Hubs or Devices

Connect 10 Mbps devices using UTP/STP Cat 3, 4 or 5 cables with RJ-45 connectors, enabling sending/receiving to or from other 10 Mbps devices. By default, each port is set as auto-sensing mode. Hub FHU-1201/1202/2401/2402TFXS can detect a 10BASE-T device and transmit/receive information to/from it.

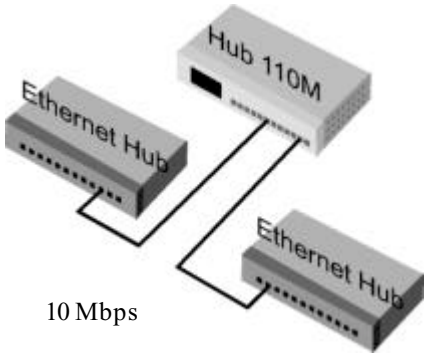


Figure 2.4 Connecting Ethernet Hubs

Connecting Fast Ethernet Switching Hubs

Connect 100 Mbps devices using UTP/STP Cat 5 cables with RJ-45 connectors, maximum length 5 meters, enabling sending/receiving to other fast Ethernet switching hubs. By default, each port is set as auto-sensing mode. Hub FHU-1201/1202/2401/2402TFXS can detect a connected 100BASE-TX device and transmit/receive information to/from it. The distance between switching hubs can be extended up to 2 km by connecting two hubs through expansion modules using fiber cable.

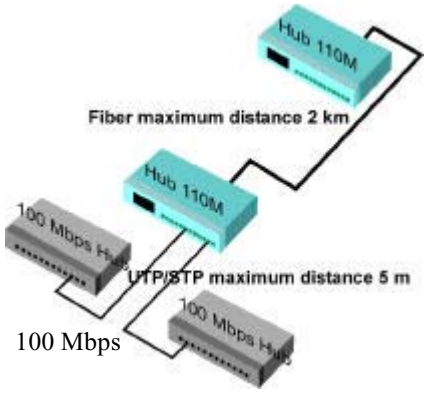


Figure 2.5 Connecting Fast Ethernet Hubs

Connecting the Other Dual Speed Hubs

Other dual speed hubs can be connected to the ports of Hub FHU-1201/1202/2401/2402TFXS. Each port can auto-sense the port speed and set its port speed to match the connected port. The maximum distance between device is 5 meters using Cat 5 UTP/STP cable. Increase the distance between dual speed hub you must use fiber cable and connect using expansion switch modules. For more information about expansion switch modules, see Chapter 3, “Using Expansion Modules”.

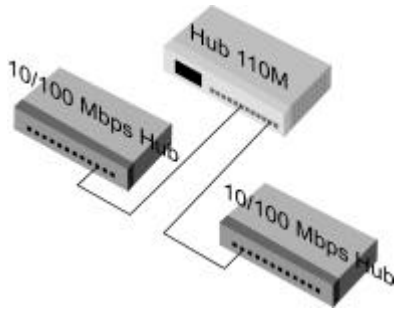


Figure 2.6 Connecting the Other Dual Speed Hubs

Chapter 3

Using Expansion Modules

Expansion Module Overview

Expansion modules provide additional functions to FHU-1201/1202/2401/2402TFXS hubs such as internal bridging of 10 Mbps and 100 Mbps segments, and extended distances between devices. Expansion modules provide an internal bridge and an external distance extender. The available modules are:

- Module MDU-0112TX
- Module MDU-0113FX
- Module MDU-0205TX
- Module MDU-0206FX

Internal Bridge Function

The Internal Bridge Function is used for bridging 10 Mbps and 100 Mbps segments in a hub or in a Hub FHU-1201/1202/2401/2402TFXS stack. Only one internal switch can be enabled in a Hub FHU-1201/1202/2401/2402TFXS stack, more than one will cause network looping.

Note: There can only be one internal switch enabled in a Hub FHU-1201/1202/2401/2402TFXS stack, however multiple external bridges are allowed.

Therefore, if more than one module exists in a Hub FHU-1201/1202/2401/2402TFXS stack ensure that only one module has its internal bridge enabled.

External Bridge Function

The external bridge function is used to extend the distance between 100 Mbps hubs or stacks from the normal limitation of five meters to one hundred meters with TX modules using RJ 45 cable. With TF modules using fiber cable, you can expand the distance between hubs or stacks up to 2km.

Backpressure (flow control)

When packets are passed from 100 Mbps segments to 10 Mbps segments the flow is restricted due to the lesser capacity of the 10 Mbps segment causing backpressure and resulting in dropped packets. With flow control or backpressure enabled, packets are made to wait until the flow is unrestricted before being sent, reducing the number of dropped packets.

Installing a Bridge Module

Power down Hub FHU-1201/1202/2401/2402TFXS before installing a bridge module. Bridge modules have both hardware and software configuration settings. The hardware configurations must be made before you physically install the module and the software configurations must be made using a master hub, after the module is installed and before the bridgeing functions will take effect. Please read this section carefully before installing modules.

To install these modules, perform the following steps.

Notes:

These modules are not hot swappable. You must remove power from the hub before installing or replacing a bridge module.

a) b) You should enable the internal bridge on only one bridge module when you have multiple bridge modules installed in a Hub FHU-1201/1202/2401/2402TFXS stack. This prevents a network loop condition.

---

c) Three bridge modules are shipped with the Internal Bridge function enabled (MDU-0112TX, MDU-0205TX and MDU-0206FX), only the MDU-0113FX is shipped with the Internal Bridge function disabled. All models shipped with the backpressure function disabled.

1. Set the bridge function and backpressure function by moving the appropriate jumpers. See the following sections for the bridge module model that you are installing and set the jumpers accordingly.
2. Remove the power from the hub by disconnecting the power cable from the AC outlet.
3. Remove the installed bridge module or blank cover of the expansion module slot (not the NMU slot, only the bottom slot is available) by turning the two knobs on the front counterclockwise as shown in Figure 3.1.

Figure 3.1 Removing the Blank Module Panel

4. Insert the new module, ensuring that the edges slide through the guides, as shown in Figure 3.2

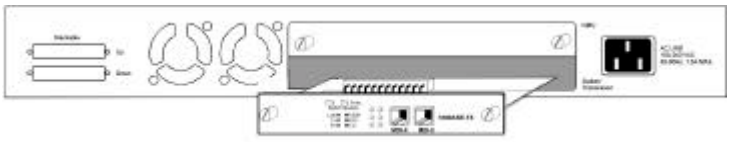


Figure 3.2 Insert the Module

5. Turn the two knobs on the new bridge mo dule until they are securely attached to the hub.
6. Connect the appropriate communication cable to the new module.
7. For stand alone slave models the installation is complete, just connect AC power.

8. If your adding this hub to an existing stack, connect the hub to the stack. See “Stacking Hubs using Daisy Chain Cables” on page 2-3.
9. Reconnect the AC power cord to the wall outlet.
10. For master models or slave models in a Hub FHU-1201/1202/2401/2402TFXS stack with a master present, you must configure the software for the installed bridge module to enable the internal bridge function because the software default setting is disabled. The default software setting will not allow the internal bridge function to enable. The software must be configured using a master hub.
11. Start a Console session and set the software configuration for the new module. For information on Bridge Module configuration settings see “Controlling Devices” on page 5-23. For informatin on starting a console session see Chapter 5 “Console Management for Hub FHU-1201/1202/2401/2402TFXS”.

TX Module LED Indicators

The LEDs on each module indicate port activity:

- **Link:** On, indicates a link is up.
- **Tx:** On, indicates a transmission in progress.
- **Rx:** On, indicates receiving data.
- **100M:** On, indicates the 100 Mbps segment is link up. Off, indicates the 10 Mbps segment is link up when Tx or Rx LED is also on.
- **FDX:** On, indicates the port is set to *full duplex*. Off, indicates the port is set to *half duplex*.
- **Collision:** On, indicates collision occurring.

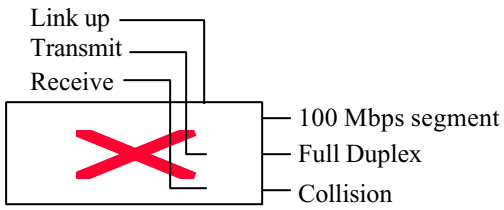


Figure 3.3 TX Module LEDs

TF Module LED Indicators

The LEDs on each module indicate port activity:

Link:	On, indicates a link is up.
Tx:	On, indicates a transmission in progress.
Rx:	On, indicates receiving data.
FDX:	On, indicates the port is set to *full duplex*. Off, indicates the port is set to *half duplex*.
Collision:	On, indicates collision occurring.

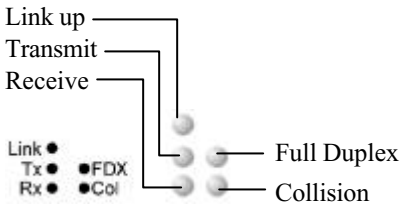


Figure 3.4 TF Module LEDs

Module MDU-0112TX

Module MDU-0112TX is either an *internal bridge* for bridging the internal 10 Mbps and 100 Mbps segments **or** an *external 10/100BASE-TX distance extender* with MDI-X and MDI-II interfaces using RJ 45 cable. Only one of these functions can be enabled at one time. The internal or external bridge must be enabled or disabled with on board jumpers before installation. Module MDU-0112TX's flow-control (backpressure) can be enabled or disabled by setting the on board jumpers before installation. The default settings are as follows:

Bridge Function setting- Internal (**Default**)

Backpressure setting- Disabled (**Default**)

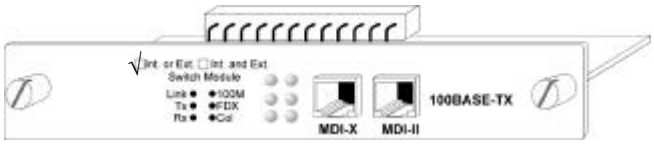


Figure 3.5 Module MDU-0112TX

Module MDU-0112TX Jumpers

The default jumper setting of the MDU-0112TX module, is internal bridge enabled. To disable the internal bridge and enable the external bridge change the jumpers (JP1~JP16) from 1&2 to 2&3.

Jumpers JP1~JP16

- 1&2 connected = internal bridge is enabled (**Default**)
- 2&3 connected = external bridge is enabled

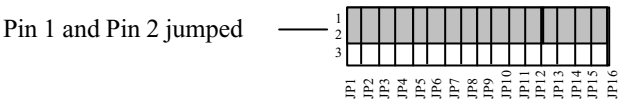


Figure 3.6 Module MDU-0112TX Bridge Jumpers

Module MDU-0112TX Backpressure Jumpers

The default jumper setting for backpressure is disabled. To enable the backpressure function, change JP18 jumper to 2&3.

Jumper JP18

- 1&2 =disabled (**Default**)
- 2&3 = enabled

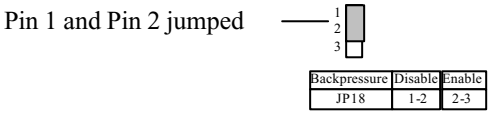


Figure 3.7 Module MDU-0112TX Backpresser Jumpers

Module MDU-0205TX

Module MDU-0205TX is a 3-port bridge module with a *two port internal bridge* for bridging 10 Mbps and 100 Mbps segments **and** an *external 10/100BASE-TX distance extender* with MDI-X and MDI-II interfaces using RJ 45 cable. Both one of these functions can be enabled at one time in fact the distance extender is always enabled. The internal or external bridge must be enabled or disabled with on board jumpers before installation. Module MDU-0205TX's flow-control (backpressure) can be enabled or disabled by setting the on board jumpers before installation. The default settings are as follows:

Bridge Function setting- Internal and External enabled (**Default**)

Backpressure setting- Disabled (**Default**)

Note: Distance Extender is always enabled in module MDU-0205TX.

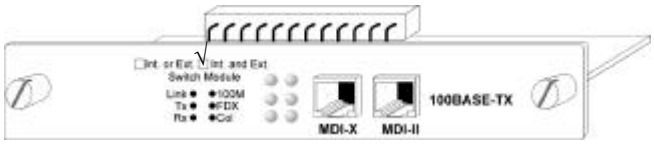


Figure 3.8 Module MDU-0205TX

Module MDU-0205TX Jumpers

The default jumper setting of the internal bridge of Module MDU-0205TX is enabled. The external distance extender is always enabled. To disable the internal bridge, change the jumpers (JP2, J4 & JP6) from 1&2 to 2&3.

Jumpers JP2, JP4 ~ JP6

- 1&2 connected = internal bridge is enabled (**Default**)
- 2&3 connected = internal bridge is disabled (**Default**)

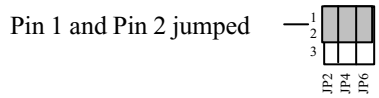


Figure 3.9 Module MDU-0205TX Bridge Jumpers

Module MDU-0205TX Backpressure Jumpers

The default jumper setting for backpressure is disabled. To enable the backpressure function, change JP1 and JP7 jumpers to 2&3.

Jumpers JP1, JP7

- 1&2 = disabled (**Default**)
- 2&3 = enabled

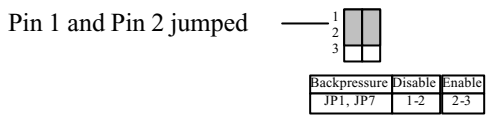


Figure 3.10 Module MDU-0205TX Backpressure Jumpers

Module MDU-0113FX

Module MDU-0113FX provides a two port *internal bridge* for bridging 10 Mbps and 100 Mbps segments **or** *100BASE-FX distance extender* with SC type connectors and fiber cable. The internal bridge must be enabled or disabled with on board jumpers before installation. The external distance extender is enabled by default. Module MDU-0113FX's flow-control (backpressure) can be enabled or disabled by setting the on board jumpers before installation. The default settings are as follows:

Bridge Function setting- Internal disabled (**Default**)

Backpressure setting- Disabled (**Default**)

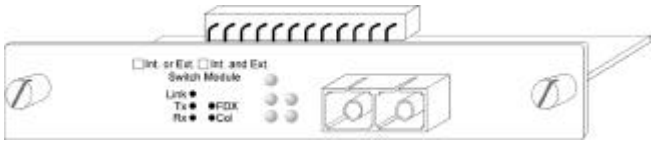


Figure 3.11 Module MDU-0113FX

Module MDU-0113FX Jumpers

The default jumpers setting of the Module MDU-0113FX is internal bridge disabled. To enable the internal bridge and disable the external bridge change the jumpers (JP2~JP17) from 2&3 to 1&2.

Jumpers JP2~JP17

- 1&2 connected = internal bridge is disabled (**Default**)
- 2&3 connected = external bridge is enabled

Pin 2 and Pin 3 jumped

Figure 3.12 Module MDU-0113FX Bridge Jumpers

Module MDU-0113FX Backpressure Jumpers

The default jumper setting for backpressure is disabled. To enable the backpressure function, change JP19 jumper to 2&3.

Jumper JP19

- 1&2 = disabled (**Default**)
- 2&3 = enabled

Pin 1 and Pin 2 jumped

Backpressure	Disable	Enable
JP19	1-2	2-3

Figure 3.13 Module MDU-0113FX Backpressure Jumpers

Module MDU-0206FX

Module MDU-0206FX provides a two port *internal bridge* for bridging 10 Mbps and 100 Mbps segments **or** *100BASE-FX distance extender* with SC type connectors and fiber cable. The internal bridge must be enabled or disabled with on board jumpers before installation. The external distance extender is always enabled. Module MDU-0113FX's flow-control (backpressure) can be enabled or disabled by setting the on board jumpers before installation. The default settings are as follows:

Bridge Function setting- Internal enabled (**Defaul**t)

Backpressure setting- Disabled (**Default**)

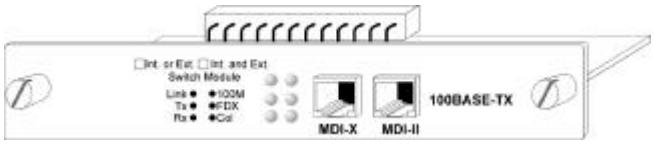


Figure 3.14 Module MDU-0206FX

The default jumper settings of the Module MDU-0206FX is internal bridge enabled. The external distance extender is always enabled. To disable the internal bridge, change the jumpers (JP3~JP7) from 1&2 to 2&3.

Jumpers JP3~JP7

- 1&2 connected = internal bridge is disabled (**Default**). The external distance extender is enabled.
- 2&3 connected = internal bridge is enabled

Pin 1 and Pin 2 jumped

Figure 3.15 Module MDU-0206FX Bridge Jumpers

Note: Distance Extender is always enabled in module MDU-0205TX.

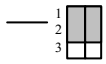
Module MDU-0206FX Backpressure Jumpers

The default jumper setting for backpressure is disabled. To enable the backpressure function, change JP2 and JP8 jumper to 2&3.

Jumpers JP2, JP8

- 1&2 = disabled (**Default**)
- 2&3 = enabled

Pin 1 and Pin 2 jumped



Backpressure	Disable	Enable
JP2, JP8	1-2	2-3

Figure 3.16 Module MDU-0206FX Backpressure Jumpers

Chapter 4

Managing Hub through Mini-Console

Mini-Console Overview

The Mini-Console is a high definition display panel that provides brilliant text and graphics. It continuously displays information about the system, port status or other information depending on the menu selected. Extensive configuration settings can be viewed and configured with the Mini-Console. The Mini-Console is only available for model Hub FHU-1202/2402TFXS.

Features

- **High definition display panel** (text and graphics)
- **Message Zone**
- **Gauge Bars**
- **% Indicators**
- **Port Indicators**
- **Port Frame Indicators**
- **Console Keys**
- **Hub ID**
- **Group Indicators**
- **Symbols** (Lock, Caution, WWW, SNMP & OOB)

Mini-Console Display Panel

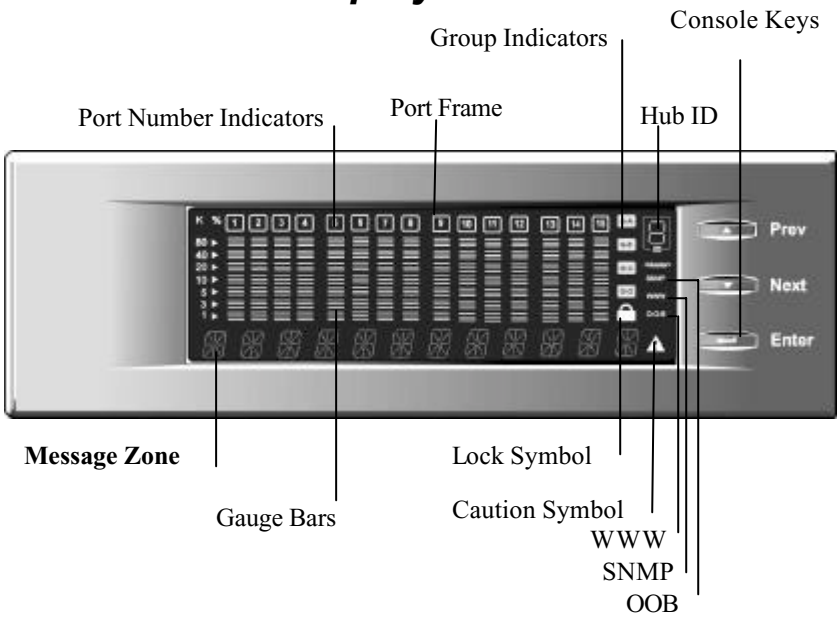


Figure 4.1 Mini-Console

The Mini-Console goes blank after approximately 60 minutes if there is no Control Key activity.

VFD Display

The Vacuum Florescent Display (VFD) displays the following port and system information:

% The relative percentage of utilization or collision.

Port Number Indicators (1 to 12)

Indicates the number of a port, and with their brightness, indicate status information. See Table 4-1.

Port Indicator Frame ( )

Indicates which ports are disabled

Message Zone

The Message Zone displays the menu items of the menu tree, port information and system information including self-diagnostic tests and error messages.

Gauge Bars

Displays information such as utilization, port status, and as an indicator for groups or ports.

Lock Icon Indicates the control panel configuration is locked.

G-A Port group indicator displays status of ports 1 to 12

G-B Ports 13 to 24

Master Indicates this hub is a master hub.

SNMP Indicates the hub is SNMP manageable.

WWW Indicates the Web Management feature is enabled.

OOB Indicates that out-of-band is enabled.

Observing Basic Port Information

The basic port information, such as link up, link down, transmit and receive activity, enabled and disabled, and auto partition can be easily spotted through the bar gauges, Messages Zone and Port Indicators located in the first row of the Mini-Console. The gauge bars below each linked port ascend and descend in relation to the amount of traffic through the ports.

Port Indicator Definition

The port number indicators define the port status and activity by the way they are illuminated, such as ON, OFF, flashing and with a frame around the numbers.

The following table summarizes the definition of the port indicators.

Port No.	Frame	Indicates
Normal	Off	Port is available but link is down.
Bright	Off	Port is available and link is up.
Bright	On	The Link is up and the administrator has disabled the port.
On	On	The Link is down and the administrator has disabled the port.
Flashing	Off	Link is up and transmitting or receiving data.
On	Blinking	The port is partitioned by machine itself due to errors.

Table 4.1 Port Indicator Definitions

Console Keys

The Console Keys are used to cycle through the menu tree, to make selections and settings. The Prev key and the Next Key cycle's one position in the same level, and the Enter key makes a selection. To move up the menu tree toward the root, select BACK or MAIN MENU in the menu tree structure.

BACK
Selecting BACK moves back up one level in the menu tree.

MAIN MENU
Selecting MAIN MENU moves directly to the main level in the menu tree.

The following table summarizes the Console Keys functions.

Prev	Cycles back through the current menu level.
Next	Cycles forward through the current menu level.
Enter	Select the displayed menu item or when pressed and held changes a setting. Holding down the Enter key changes the default setting and places an "*" before the item indicating it is the current default.

Table 4.2 Console Keys

Menu Tree

The menu tree consists of these seven main level menus:

- **Utilization**
- **Group Select**
- **Statistics**
- **Port Status**
- **Port Configuration**
- **Unit Configuration**
- **System Information**

The Main Menu items and their sub menus are shown in below.

UTILIZATION	Press "ENTER" to toggle port menus 1-12 or 13-24

GROUP SELECT	GROUP 1~GROUP *N*

STATISTICS	PORT 1~PORT *N*	READABLE FRM
		READABLE OCT
		FCS ERRORS
		ALIGN ERRORS
		FRM TOO LONG
		SHORT EVENTS
		RUNTS
		COLLISIONS
		LATE EVENTS
		VERY LONG EN
		RATE MISMTCH
		AUTO PART
		TOTAL ERRORS

PORT STATUS	ALL PORTS	10M PORTS
		100M PORTS
		LINK UP
		LINK DOWN
		POLAR NORMAL
		POLAR REVERS
		NO AUTO PARTS
		AUTO PART
		ENABLE
		DISABLED
	PORT 1~PORT N	Press “ENTER” to show the status applied to the port

PORT CONFIG	ALL PORT	ENABLED
	PORT 1~PORT N	DISABLED
		AUTO-NEGO
		10BASE-T
		100BASE-X

UNIT CONFIG	CONSOLE LOCK	LOCK	
	NETWORK CONFIG	IP ADDRESS	
		SUBNET MASK	
		DEF GATEWAY	
	SET PASSWORD		
	SYS RESTART	CONTINUE	
		CANCEL	
	SYS DEFAULT	CONTINUE	
		CANCEL	
	EIA232 CONFIG	BAUD RATE	1200
			2400
			4800
			9600
			19200
			38400

SYSTEM INFO	HW VER	*HW version is displayed*
	SW VER	*SW version is displayed*
	IP ADDRESS	*IP Address is displayed*
	SUBNET MASK	*Subnet Mask is displayed*
	DEFAULT GATEWAY	*Default Gateway is displayed*

Observing Network Traffic

You can observe the network traffic in the Mini-Console with the Utilization menu. Seven columns of gauge bars, which shift continuously from left to right as time elapses, represent the utilization rate of each segment. The gauge bars columns on the left are the most updated traffic for 10M segment and 100M segment separately. Each column of gauge bars is a historical view of the total utilization in the 10M segment and the total utilization in the 100M segment at the time the statistics were taken by the hub. The total utilization history, represented by the seven columns in each segment is over a three-second time frame.

"**UTILIZATION**" and "**10M 100M**" are displayed in the Message Zone interchangeably at intervals of several seconds as shown in Figure 4.2 and Figure 4.3.

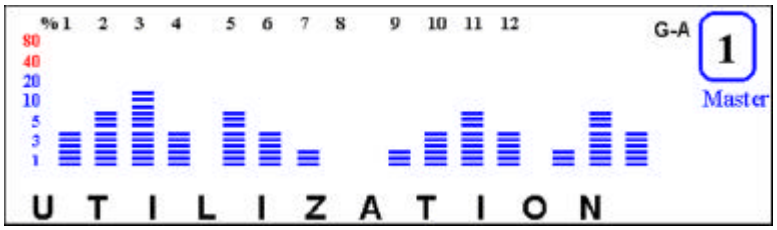


Figure 4.2 Utilization per Port

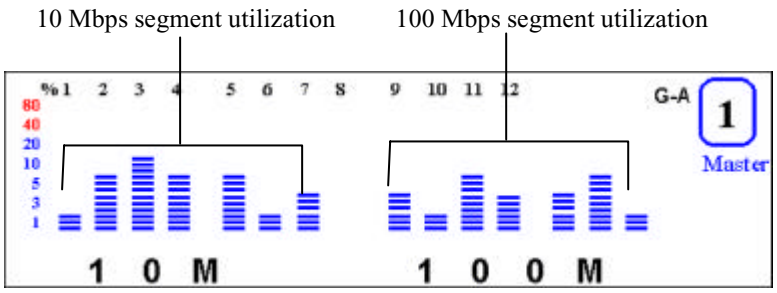


Figure 4.3 Utilization per Segment

Selecting Group

You can select a group to monitor and configure when there are managed hubs, daisy chained to the master hub. “Group” refers to a hub in the stack, the range is 1~6 when the maximum number of hubs exist in the stack. You can manage each hub using the Mini-Console. To select a group:

1) From the main menu press <**Next**> until “**GROUP SELECT**” is displayed in the Message Zone.

2) Press <**Enter**>. Several bars under the Port number indicate the current group, as shown in Figure 4.4.

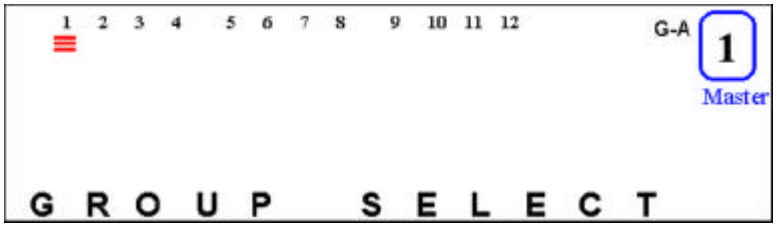


Figure 4.4 Group Select

3) Press <**Next**> until the group number you wish to monitor is displayed in the Message Zone as shown in Figure 4.5, and Figure 4.6.

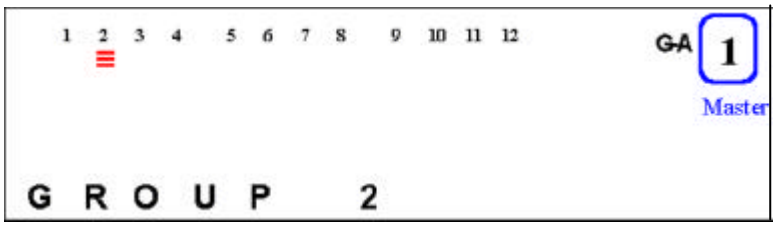


Figure 4.5 Group 2

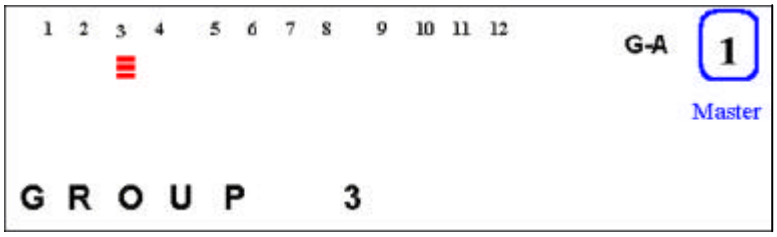


Figure 4.6 Group 3

Monitoring Port Statistics

You can monitor statistics of individual ports or all ports simultaneously using the Statistics Menu. Table 4.3 “Port Statistics Counters” lists the available counters that can be monitored.

Counter Type	Displayed
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 bad Frame Check Sequence.
ALIGN ERRORS	The total number of packets received that have bad FCS with a non-integral number of octets.
FRM TOO LONG	The total number of packets that were received that were longer than 1518 octets (including FCS octets but excluding framing bits) and were otherwise well formed.
SHORT EVENTS	The total number of packets that were received that were less than 64 octets (including FCS octets but excluding framing bits) and were otherwise well formed.
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 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 was greater than the ValidPacketMinTime event and also frequency (data rate) is delectably mismatched from the local frames mismatch frequency.
AUTO PART	Total number of times the port was 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.

Table 4.3 Port Statistic Counters

Selecting a port to monitor

1) Press <**Next**> until Statistics is displayed in the Message Zone.

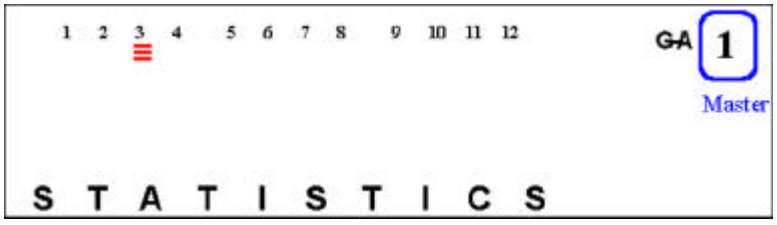


Figure 4.7 Statistics

2) Press <**Enter**> to go to port selection menu and select a port for viewing. In the port selection menu, six units of the gauge bars, below the port number, indicate the current port. The current port number is displayed in the Message Zone, as shown in Figure 4.8.

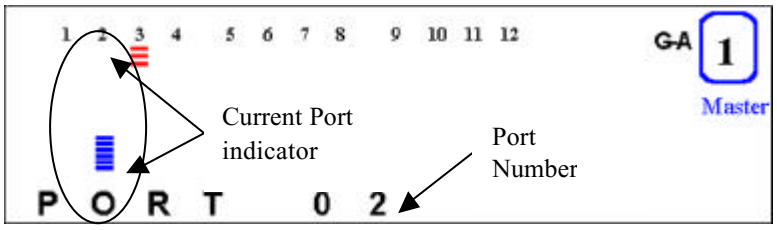


Figure 4.8 Port Indicator Guage Bars

3) Press **<Next>** to move the "port cursor" to the desired port, the port number is displayed in the Message Zone, as shown in Figure 4.9.

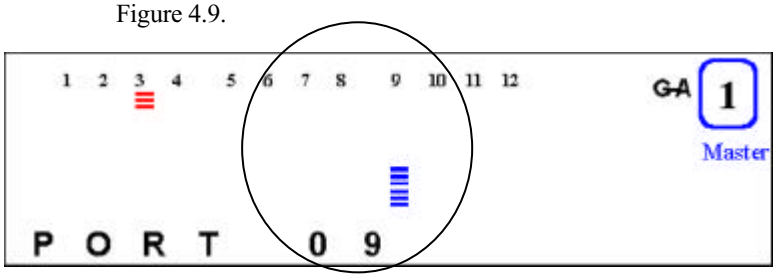


Figure 4.9 Scrolling to a Port

4) Press **<Enter>** to confirm the selection of the port; and go to the counter type selection menu. The name of the port statistics counter "READABLE FRM" is displayed in the Message Zone as shown in Figure 4.10.

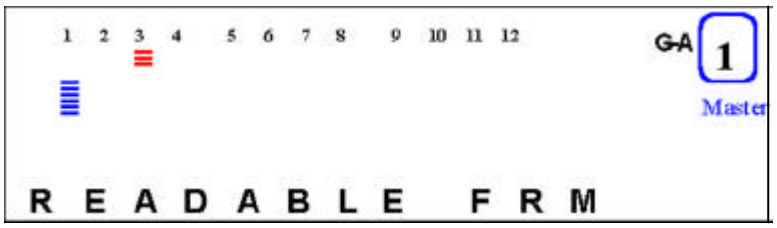


Figure 4.10 Readable Form

5) Press **<Next>** to scroll through each type of counter.

6) Press **<Enter>** to view the value of the current counter (currently displayed in the Message Zone), the value of the counter is displayed in the Message Zone.

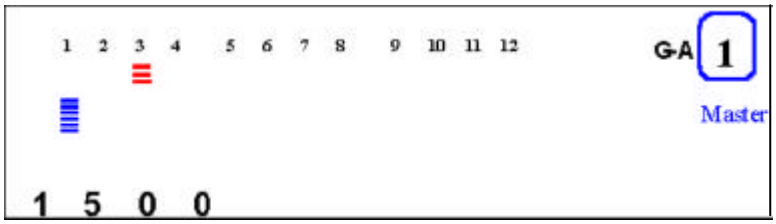


Figure 4.11 Statistic Counter Value

Monitoring Port Detail Information

You can monitor detailed port information for all ports at once or individual port using the Port Status menu.

Monitoring All Ports Status

To view all port status:

1) Press <**Next**> until "PORT STATUS" is displayed in the Message Zone. The current selected group is indicated by the group cursor under the port ID indicator, as shown in Figure 4.12.

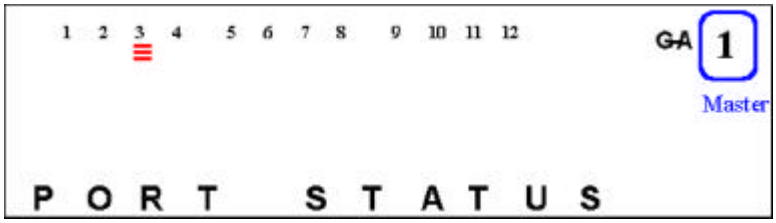


Figure 4.12 Port Status

2) Press <**Enter**>. "ALL PORTS" is displayed in the Message Zone. When monitoring all ports, the gauge bar columns are divided into 24, one for each port. The upper row of columns represents ports 13~24 and the lower row of columns represents ports 1~12.

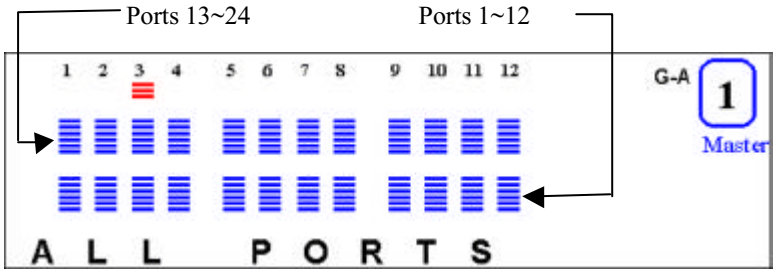


Figure 4.13 All Ports Status

3) Press <**Enter**> to view all the ports' status at once. Figure 4.14 illustrates 10M ports. In Figure 4.14, ports 13, 14, 15, 16, 19 & 22. Ports 1, 2, 3, 4, 7 & 10 are indicated as 10M ports.

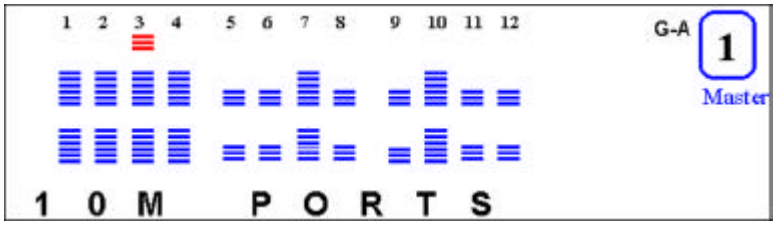


Figure 4.14 10 Mbps Ports

4) Press <**Next**> to view the status of other ports. 100M ports status is displayed. In Figure 4.15, ports 17, 18, 20, 21, 22, 24, 5, 6, 8, 9, 11 & 12 are indicated as 100M ports.

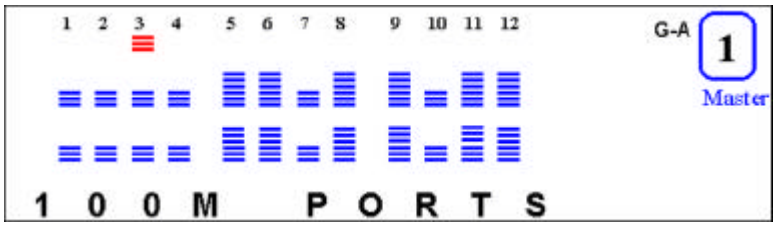


Figure 4.15 100M Ports

5) Press <**Next**> to view other port status information. The status information that is available to monitor is listed in Table 4.4.

10M PORTS	Indicates all 10M ports.
100M PORTS	Indicates all 100M ports.
LINK UP	Indicates all Link up ports.
LINK DOWN	Indicates all Link down ports.
POLAR NORMAL	The receive (Rx) polarity of the port is normal.
POLAR REVERSE	The receiver (Rx) polarity has been automatically crossed by the hub.
NO AUTO PART	Indicates all ports not auto partitioned.
AUTO PART	Indicates all Auto Partitioned ports.
ENABLED	Indicates all Enabled ports.
DISABLED	Indicates all Disabled ports.

Table 4.4 ALL PORTS Status Information

Monitoring Individual Port Status

To view the status of individual ports:

1) Press <**Next**> until “PORT STATUS” is displayed in the Message Zone.

2) Press <**Enter**> to go to the port selection menu. “ALL PORTS” is displayed in the Message Zone.

3) Press <**Next**> to select an individual port. “PORT 1” is displayed in the Message Zone. After a slight delay the status of Port 1 is automatically cycled through, displaying the status of Port 1.

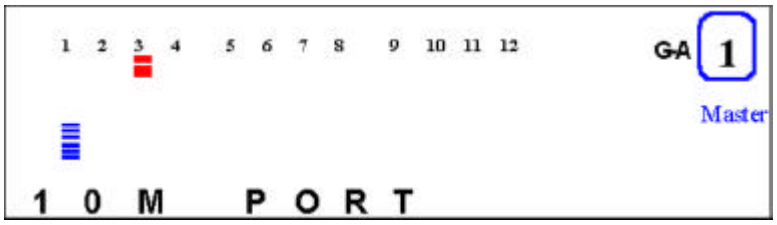


Figure 4.16 Port Status

4) Press **<Next>** to view port status of the next port. After a slight delay the status of the selected port is automatically cycled through, displaying the status of the selected port.

5) Press <**Next>** to view port status of other ports.

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. The ports must be configured to match the devices at the other end of the link. Settings such as speed must be identical. All ports are set to default to AUTO NEGO. When the AUTO NEGO mode is set, 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 current selected hub is indicated by the “group cursor” under the port number indicator, as shown in Figure 4.17.

Figure 4.17 Port Configuration

Configuring ALL PORTS:

1) With "PORT CONFIG" displayed in the Message Zone, press **<Enter>** to go to the port selection menu. "All PORTS" is displayed in the Message Zone.

2) Press <**Enter**>. The first of the configuration items for all 24 ports is indicated in the Message Zone. Press <**Next**> to scroll through all the configuration options. Figure 4.18, illustrates the ports that are set to Auto Negotiate enable, indicated by the columns that have 6 gauge bars, specifically ports 5, 6, 8, 12, 17, 18, 19, 24. Columns that have only 3 gauge bars indicate the ports that are not set to the configuration displayed in the Message Zone. To change the configuration scroll to the desired setting and press and hold the ENTER key. The new setting will display 6 gauge bars for all ports.

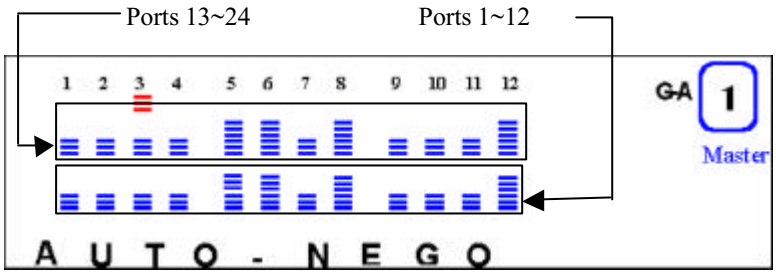


Figure 4.18 Auto Negotiate Ports

3) Press **<Next>** to scroll through each configuration item.

4) Press **<Enter>** to apply the configuration displayed in the Message Zone to all the ports.

Configuring a single port

1) With "PORT CONFIG" displayed in the Message Zone, press <**Enter**> to go to the port selection menu.

2) Press the <**Next**> to select an individual port.

3) Press <**Enter**>. The configuration of the selected port is displayed in the Message Zone. Six gauge bars below the port number indicate the current port. 3 gauge bars (group cursor) directly under the port number indicate the current group.

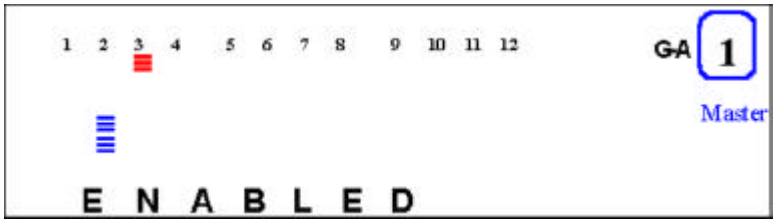


Figure 4.19 Current Configuration

4) Press <**Next**> to scroll through each configuration item.

5) Press <**Enter**> to apply the currently displayed configuration to the port.

The applied configuration is indicated by an asterisk sign displayed before the name of the configuration in the Message Zone as shown in Figure 4.20, otherwise, the asterisk sign will not appear.

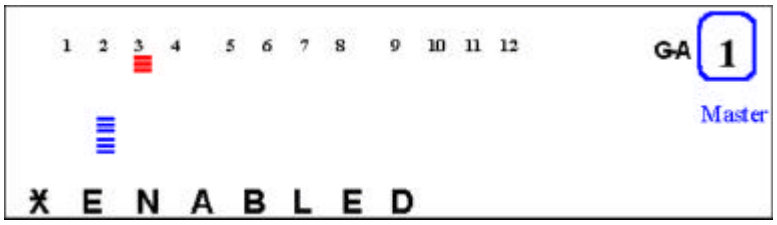


Figure 4.20 Current Port Configuration (single port)

Table 4.5 lists typical default settings and the possible optional settings for a port. An "*" appears before each current setting. To change a setting press and hold down <**Enter**> until an "*" appears before the setting, the "*" is removed from the previous setting.

Default	Optional settings
*AUTO-NEGO	10BASE-T/100BASE-X
*ENABLE	Disable

Table 4.5 Port Setting

Unit Configuration

You can configure the hub using the Unit Configuration Menu. For security reasons you are prompted for password when the device is locked. Without the password users cannot enter the Unit Configuration menu in order change any unit configurations. When the device is unlocked, no password verification is required to change the unit configurations. The password entry is described in "Set Password", on page 4-25.

Configuring the unit

1) Select UNIT CONFIGURATION from the Main Menu.

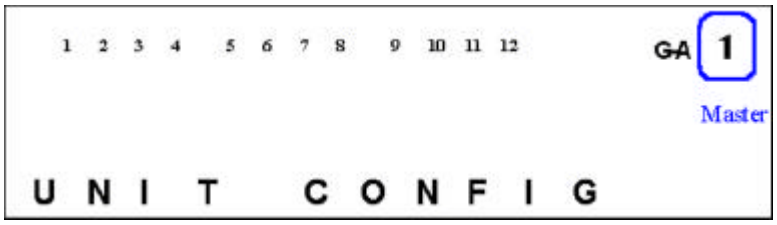


Figure 4.21 Unit Config Main Page

2) Press the **<Enter>** to go to the UNIT CONFIGURATION menu.

3) Press the <**Next**> to scroll through each configuration option.

4) Press <**Enter>** to go to the next level of configuration menu.

Table 4.6 lists Unit Configuration options.

Console Lock	Enable/Disable
Network Config	IP Address, Subnet Mask and Default Gateway
Set Password	Set new password
System Restart	Restart hub.
System Default	Reset hub to factory configuration
EIA232 Config	Baud Rate

Table 4.6 Unit Configuration Options

Lock the Mini-Console

In the console lock configuration menu, the text string “LOCK” is displayed in the Message Zone. If the device is currently locked, a lock symbol is also displayed on the right side of the Mini-Console.

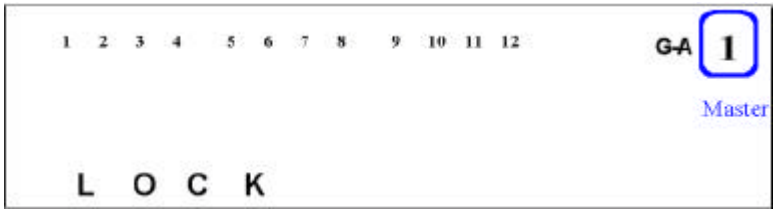


Figure 4.22 Unlocked State

1) Select UNIT CONFIGURATION from the Main Menu.

2) Press the **<Enter>** to go to the UNIT CONFIGURATION menu.

3) Console Lock is displayed in the Message Zone.

4) Press **<Next>** to toggle the lock/unlock state.

5) Press **<Enter>** to set the configuration, a lock sign will appear in the display.

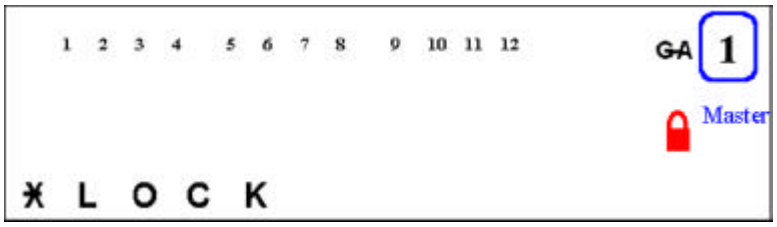


Figure 4.23 Locked State

Unlock the Mini-Console

Once unlocked, a password is not required, to make configuration settings with the Mini-Console. The console will return to the Lock State after 15 minutes of no key activity. The default password is “0000”. To unlock the Mini-Console:

1) Select UNIT CONFIGURATION from the Main Menu.

2) Press the **<Enter>** to go to the UNIT CONFIGURATION menu.

3) You are prompted to enter the password.

4) Enter the password. The console is unlocked.

Network Configuration

The Network Configuration menu allows setting the hub's IP Address, Subnet Mask and Default Gateway. The hub's Network Configurations must be set to compatible settings with LAN configurations to make connections to the hub.

Configuration	Default
IP ADDRESS	000.000.000.000
SUBNET MASK	000.000.000.000
DEFAULT GATEWAY	000.000.000.000

Table 4.7 Network Configuration

IP Address Configuration

1) Select "UNIT CONFIG" and press <**Enter**>.

2) Press <**Next**> until "NETWORK CONFIG" is displayed in the Message Zone.

3) Press <**Enter**>. IP ADDRESS is displayed in the message zone.

4) Press <**Enter**>. The current IP address is displayed in the IP address configuration menu. The first digit is blinking.

Note: the IP address is too long to be fully displayed and it will move to the left as digits are entered.

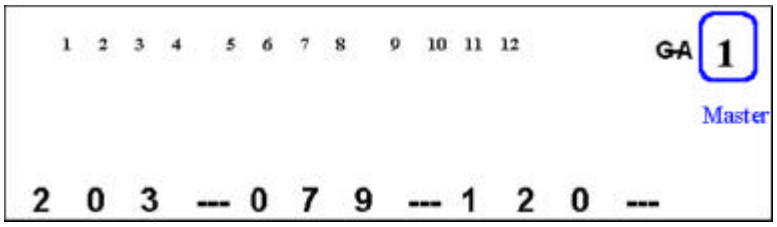


Figure 4.24 IP Address

5) Press **<Prev>** to increase the digit ("0" ~ "9").

Note: Use "0" for a blank space, for example: entering "000" equals "0" or entering "022" equals "22".

6) Press **<Enter>** to set the digit and move the cursor to the next digit. The current digit is blinking.

7) Repeat steps 1 & 2 until the entire IP address is entered.

8) Press <**Enter**> to confirm.

Since the Message Zone can not contain the whole IP address, the digits will shift to the left to make room for the last digits. When setting the IP address is complete, the system will validate the IP address. If the IP address is valid, the display will show the IP address, and the system will apply the setting. Otherwise, the system will reject it, and a message "INVALID IP" is displayed for a few seconds, and the invalid IP address is displayed again to allow modification to it.

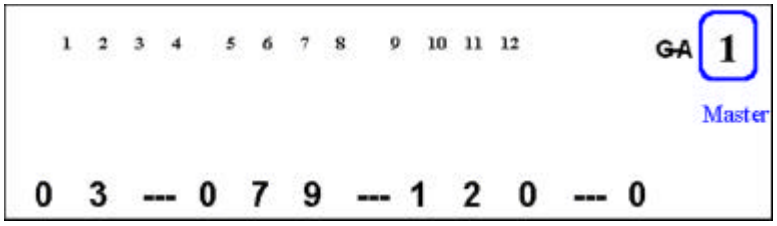


Figure 4.25 IP Address shift left

Subnet Mask

Select the SUBNET MASK option and follow the same procedure for setting an IP Address.

Default Gateway

Select the DEFAULT GATEWAY option and follow the same procedure for setting an IP Address.

Out-of-Band Configuration

You can set the out-of-band configuration with the EIA232 Config Menu, which allows settings the baud rate for the EIA232 port. Possible baud rates are 1200, 2400, 4800, 9600, 19200 or 38400.

1) Scroll to UNIT CONFIG and press **<Enter>**.

2) Scroll to EIA 232 CONFIG and press **<Enter>**.

3) Scroll to BAUD RATE and press **<Enter>**

4) Press <**Next**> until the baud rate that you want to set is displayed in the message zone.

5) Press <**Enter**> to set the new baud rate. A "*" appears before the set baud rate.

6) Press <**Next**> until BACK is displayed in the message zone.

7) Press <**Enter**> to move back up the menu tree one level.

Securing the Hub

The hub can be secured with the use of a password and the console lock. When it is locked, no configuration settings can be made, a lock icon is displayed in the Mini-Console panel and it can only be unlock by entering the correct password. The default password is "0000".

Set Password

The current password is displayed in the password setting menu. The password is displayed as four asterisks. The current digit blinks, indicating it can be configured.

1) Scroll to UNIT CONFIG and press <**Enter**>. You are prompted to enter the password, ****** PSW** appears in the message zone and the first "*" flashes. Press **<Next>** to increase the digit.

2) Unlock the control panel by entering the default password 0000, one digit at a time by pressing **<Next>** once and <**Enter**> once to progress to the next digit.

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

4) Scroll to SET PASSWORD and press <**Enter**>.

5) Enter a new password and press <**Enter**> to exit the password configuration, SET PASSWORD is displayed in the message zone.

6) Press **<Next>** until MAIN MENU is displayed in the message zone and <**Enter**> to exit to the main menu.

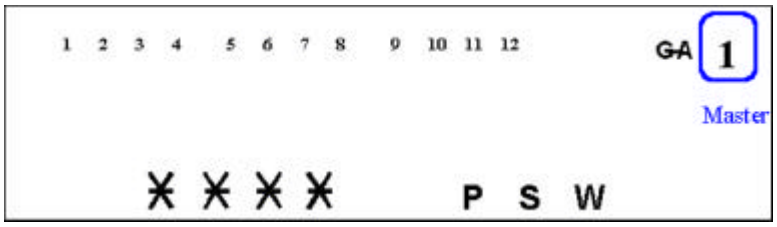


Figure 4.26 Password

Cancel Password

The password can be cancelled only by entering a new password or by setting each digit to "*".

In Case You Forget Your Password

If you forget your password, use the Console Management program to read the password setting. See Chapter 5, “Connecting the Hub via Console Interface” and “User Authentication Menu” for more information.

Restart the Hub

In the system restart menu, you can restart the system with your configurations. The hub will then use your configurations to set up the system when it restarts.

1) Scroll to UNIT CONFIG and press **<Enter>**.

2) Scroll to SYS RESTART and press **<Enter>**.

3) Press **<Enter>** at “CONTINUE” or press **<Next>** to abort the action at the menu option “CANCEL”.

4) Press **<Enter>** to confirm.

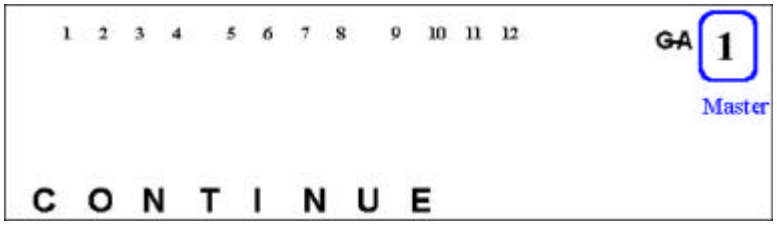


Figure 4.27 System Restart-Continue

Restore System Default Settings

The factory default configurations are selected from the SYS DEFAULT menu, a sub menu of the Main Menu item “UNIT CONFIG”. The factory

defaults are the settings that were set at the factory before shipping the hub. Restore the default settings with the following steps:

1) Press **<Enter>** at the "SYS DEFAULT" menu option. "CONTINUE" is displayed in the Message Zone.

2) Press **<Enter>** to restore factory defaults or press <**Next**> to scroll to CANCEL and press **<Enter>** to cancel the operation.

Caution: Restoring the system default settings overwrites all custom settings, including password, port configurations, and unit configurations.

About the Hub

The System Information menu displays information about the device version, the device software version, and the network configuration settings (IP Address, Subnet Mask and Default Gateway.

System Information

The following system information is cycled through in the Mini-Console:

HW VER	Hardware Version
SW VER	Software Version
IP ADDDRESS	IP Address
SUBNET MASK	Subnet Mask
DEF GATEWAY	Default Gateway

Table 4.8 System Information

Chapter 5

Console Management for Hub FHU-1202/ 2402TFXS

This Chapter is only for Hub FHU-1202/2402TFXS master hub configuration and management. When installing Hub FHU-1202/2402TFXS the first time, it is necessary to configure the hub through the Console Interface.

Connecting the Console Interface

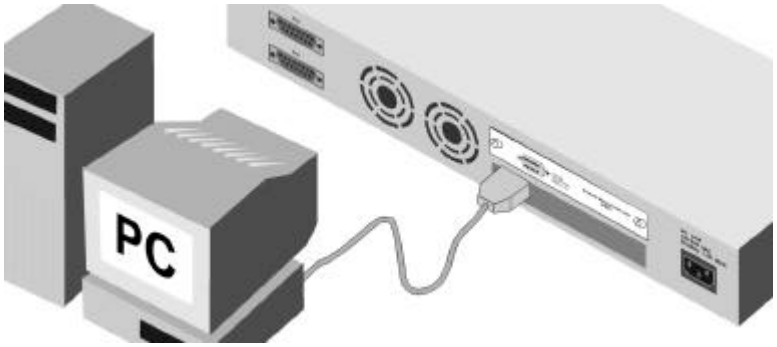


Figure 5.1 Connecting to the Console Interface

You can set up a management session by connecting a direct null modem cable between the management port on the Hub FHU-1202/2402TFXS and the communication port of your PC or terminal.

To connect a local terminal to the Hub FHU-1202/2402TFXS, perform the following steps:

1. Install a terminal emulation application such as Windows Hyperterminal on your PC.
2. Configure the terminal emulation application as follows:

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

Table 5.1 VT-100 Configuration

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.
4. Connect the console management port on the Hub FHU-1202/ 2402TFXS to your PC or DTE device using a serial cable. The Hub FHU-1202/2402TFXS has a 9-pin, male connector.
5. Press **ENTER** 2 or 3 times and the login panel to the management interface and loggin menu appears as shown in Figure 5.3. See Menu Convention in the next section to understand the menu fields and commands of the the console management interface

Menu Convention

This section describes the types of fields and commands of console management menus and their usage.

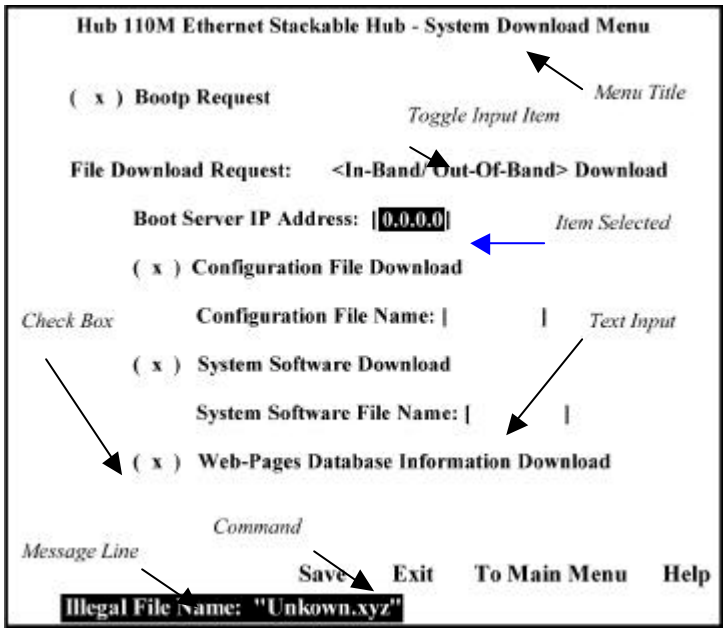


Figure 5.2 Menu Conventions

You can move the cursor between items in menus using the Tab key or arrow keys. Console Management Menu conventions are listed below.

Menu Title

The menu title briefly describes the purpose of the menu.

Check Box

Use to set a configuration item that is enclosed in round brackets “( )”. You can toggle this field to checked or not checked. Checked items are enabled and the procedure associated with this field will be performed.

Toggle Input Item

Use the space bar to toggle between options that are enclosed in angle brackets “< >”.

Text Item Item

Text fields appear between square brackets “[ ]”,and the text of the selected item can be edited or entered from the keyboard.

Item Selected

Items that are selected are highlighted. Use the Tab key to select a different item.

Commands

Available commands for a given menu, once highlighted, are executed with the Enter key.

Message Line

Displays messages prompting you confirm an action or advise that an action cannot be performed.

Using the Console Program

Ensure that the VT-100 compatible terminal parameters are set. Start the VT-100 compatible terminal and connect power to the hub. If the hub is already powered, hit <**Enter**>, one or more times to bring up the login menu. The login menu appears similar to the illustration in Figure 5.3.

Logging In

When logging in for the first time, enter the User Name as “hub” and press <**Enter**>. User Names and Passwords are not case sensitive.

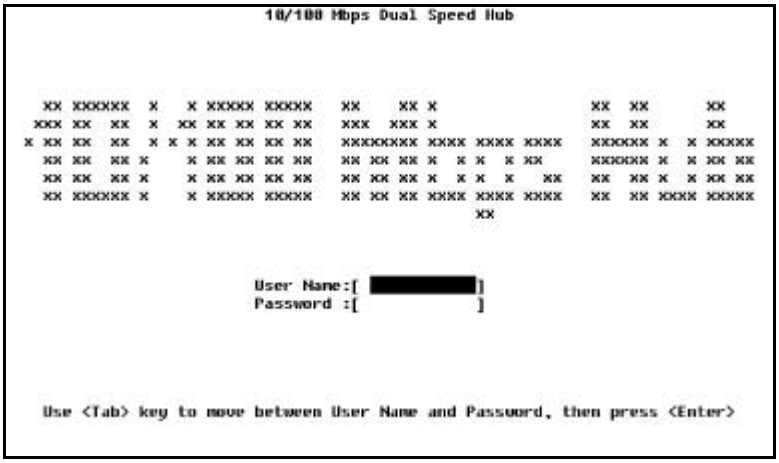


Figure 5.3 Login Menu

For security reasons, you can change the login User Name and Password. For more information about setting user names and passwords see “Users Authentication Menu” on 5-58.

Main Menu

The management functions of Hub FHU-1202/2402TFXS are available from the Main Menu. A management function is selected by pressing <**Tab**> or Up/Down **Arrow** keys to highlight the function of interest and pressing <**Enter**>. The Main Menu appears with the first item highlighted as in Figure 5.4, “Main Menu”.

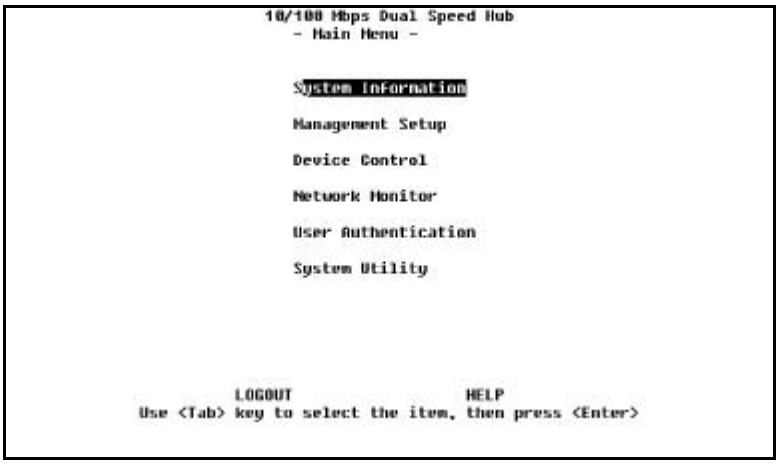


Figure 5.4 Main Menu

The Main Menu has six major selectable items: System Information, Management Setup, Device Control, Network Management, User Authentication, and System Utility.

System Information

Allows you to view general system information as well as specifying 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.

Monitoring System Information

The System Information Menu displays information about the system. You can view the system software and hardware information and configure the system configurations shown in Figure 5.5.

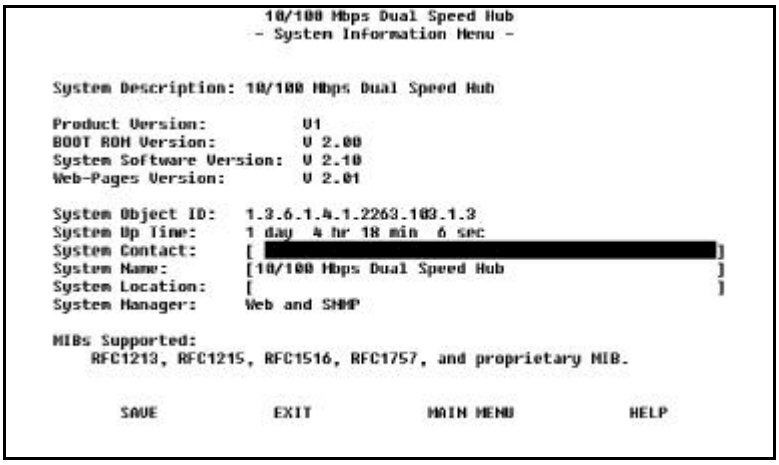


Figure 5.5 System Information

You can specify up to 48 alphanumeric characters each for the System Name, Contact, and Location to provide useful information to all users concerning HubFHU-1201/1202/2401/2402TFXS. The information on this panel should be kept current so that persons requiring assistance know whom to contact.

Note: You must select **Save** to save any changes you have made.

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 contained in the entity. 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 Up Time

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

System Contact

You can enter a name or other description of whom to contact in case of network problems. You can enter a character string up to 64 bytes.

System Name

You can enter a name or other description the hub or stack. You can enter a character string up to 64 bytes.

System Location

You can enter a name or other description of the physical location of the hub, for example the building or address, the city, etc. You can

enter a character string up to 64 bytes.

Setting up for Management

The Management Setup Menu is used to configure Hub FHU-1202/ 2402TFXS for the available management functions.

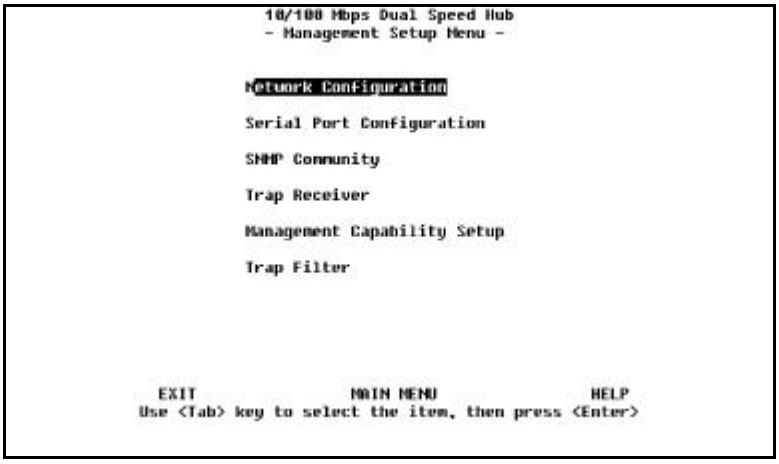


Figure 5.6 Management Setup Menu

Network Configuration

Allows you to configure the IP Address, Subnet Mask, Default Gateway, and SLIP Address.

Serial Port Configuration

Allows you to configure the serial port connections.

SNMP Community Setup

Configure community names and access right.

Trap Receiver

Set up community trap addresses.

Management Capability Setup

Enable or Disable Web access and Out-Of-Band Management.

Trap Filter

Enable or disable trap filters.

Network Configuration

There are several ways or Network Interfaces that you can use to configure FHU-1202/2402TFXS. You must setup the hub using Local Console management to enable the other management capabilities:

- Mini-Console (see Chapter 3)
- Local Console/Remote Telnet
- Web-Based Management
- SNMP Management

The Network Configuration Menu allows setting up Ethernet and SLIP connections to the hub. Network Interface <1> is used to configure Ethernet connections and Network Interface <2> is used to configure SLIP connections.

Local Console/Remote Telnet-Ethernet

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 IP Address and Subnet Mask to work with your LAN settings before you can make an Ethernet connection.

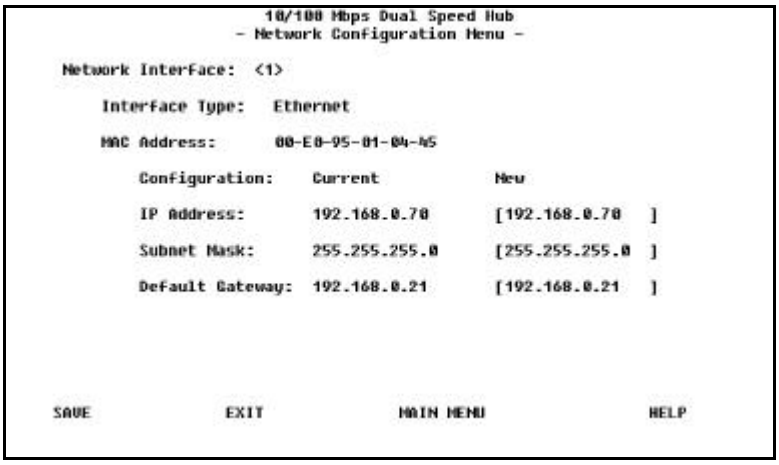


Figure 5.7 In-Band Ethernet Configuration Menu

Interface
The current interface number; 1=Ethernet, 2=SLIP

Interface Type
The interface type; Ethernet or SLIP

MAC Address
Displays the hubs MAC Address, for example; 00-E0-95-00-00-05.

IP Address
The dotted decimal address assigned to the Hub FHU-1202/ 2402TFXS.

Subnet Mask
The dotted decimal subnet mask assigned to the Hub FHU-1202/ 2402TFXS.

Default Gateway
The dotted decimal IP address of the default gateway assigned to Hub FHU-1202/2402TFXS. Hub FHU-1202/2402TFXS must be restarted before the IP address, subnet mask, and default gateway can take effect. To ensure the new information is correct, a “ping” should be done from another device connected to the Hub FHU-1202/2402TFXS.

NOTE: The hub does not respond to ping packages that are greater than 1484 bytes.

Local Console/Remote Telnet-SLIP

SLIP connections enable monitoring and configuring the Hub FHU-1202/2402TFXS remotely with a modem. To make SLIP connections use Network Interface <**2**> and set the configurations shown in Figure 5.8.

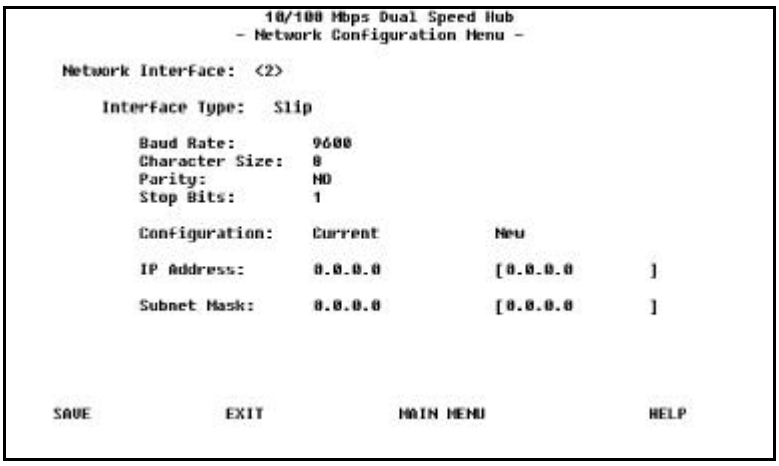


Figure 5.8 Out-of-band serial configuration Menu

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

Baud Rate

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

Character Size

8 bits character size

Parity- None

Stop Bits- 1 stop bit

IP Address:
The dotted decimal address assigned to the SLIP interface of Hub FHU-1202/2402TFXS.

Subnet Mask:
The dotted decimal mask assigned to the SLIP interface of Hub FHU-1202/2402TFXS.

Serial Port Configuration

The Serial Port Configuration Menu is used to configure Console Mode connections to VT-100 terminal emulator and Out-Of-Band serial connections to a modem.

Console Mode

To view the Console Mode settings, select “Console” Mode in the Serial Port Configurations. Console Mode settings are read only. Use the settings as shown in Figure 5.9.

Figure 5.9 Console Operation Mode

Out-Of-Band Mode

Out-of-band mode enables setting up serial port configurations for making a connection to the hub using a modem.

To make Out-Of-Band serial connections use the Out-Of-Band operation mode, in the Serial Port Configurations Menu shown in Figure 5.10.

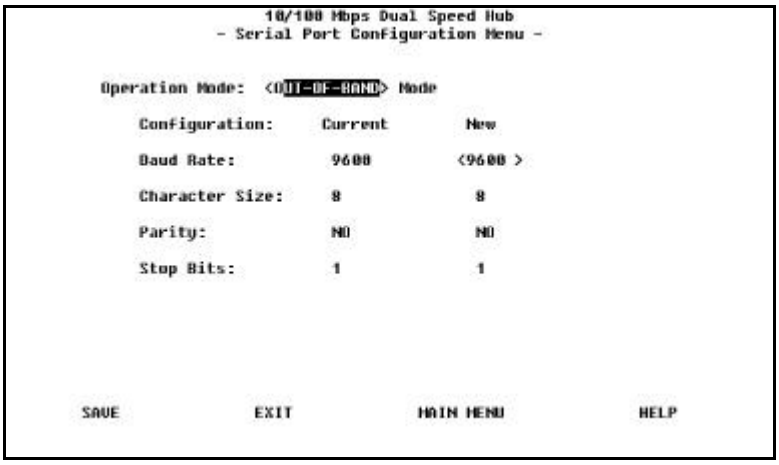


Figure 5.10 Out-of-band Operation Mode

Baud Rate

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

Character Size

8 bits character size

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. OOB also appears on the lower right side of the Mini-Conosle.

SNMP Community Setup

The SNMP Community Setup Menu used to setup SNMP communities. Up to six Community Names, Access Right, and Status can be configured.

You can add, delete, or edit SNMP community names, set the access right and status. Community names *are case sensitive*, Private and private are considered different. You cannot enter the same name more than once, an error message appears at the bottom of the panel, hit the **Esc** key to continue.

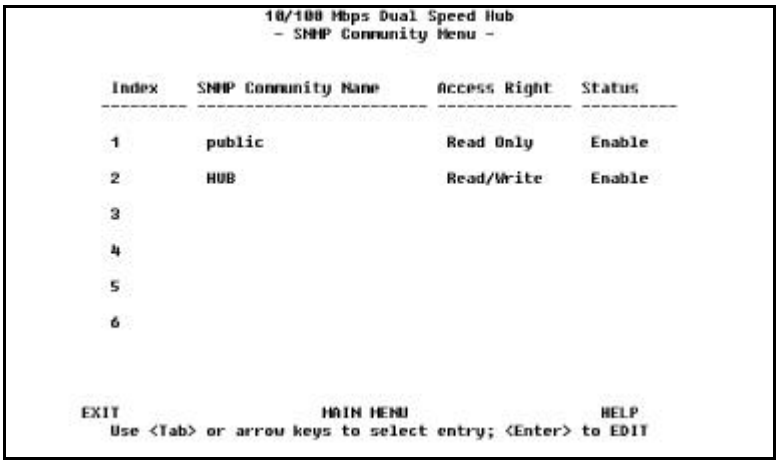


Figure 5.11 SNMP Community Setup

Community Name

Text string 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
The SNMP Community is enabled or disabled.

To add a community name:

1. Highlight an index number and press **Enter.** An editable panel is presented as shown in Figure 5.11 “SNMP Community Menu -2,” on page 5-17.
2. Enter a name in the Input field.
3. Set the access right and status
4. Highlight **ADD**, and press **Enter**, the new name is entered and displayed.

To edit a community name:

1. Enter an existing name in the Input field and press **Enter**.
2. Change the access right and status.
3. Highlight **Delete** and press **Enter** to Delete an existing name.
4. Highlight **Update** and press **Enter**.

Trap Receiver Setup

Traps are messages sent across the network to an SNMP Network Manager. These messages alert the network manager for network management purposes. You can set up six trap receivers.

You can configure the following:

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 community name can be active or inactive. Community names that are set to active will receive traps.

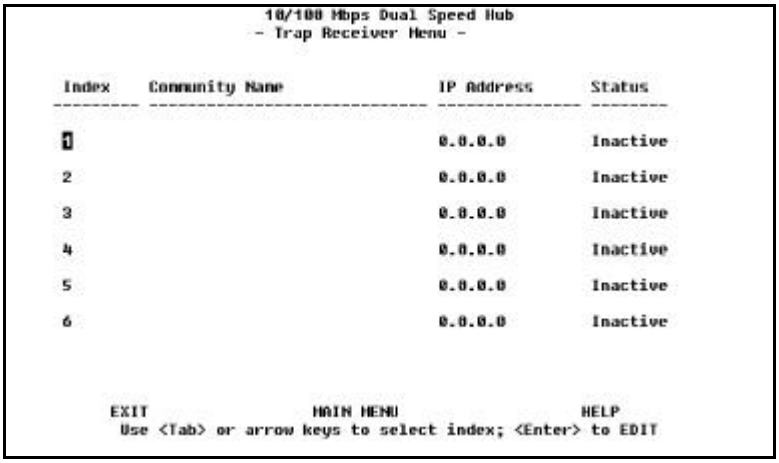


Figure 5.12 Trap Receiver Setup

To setup a trap receiver community name:

Select a Trap Community Name and press <**Enter**> to open the configuration menu for the selected index as shown in Figure 5.13.

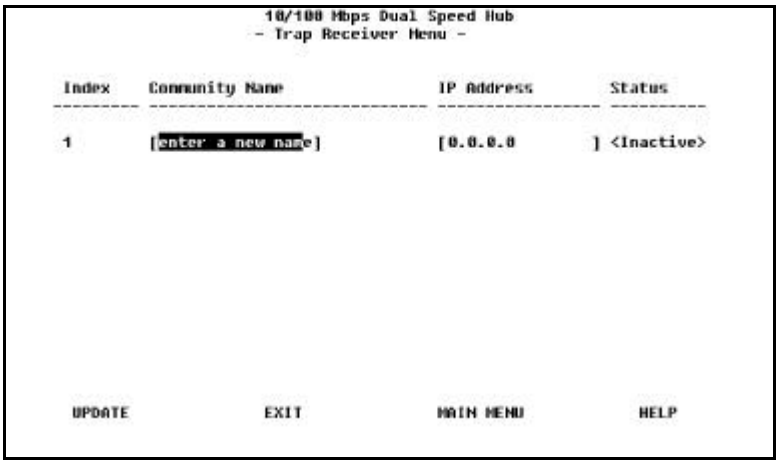


Figure 5.13 Configuring a Community Name

The Community Name can be edited, the IP Address can be configured, and the Status can be set to active or inactive. Communities that are set to *Inactive* do not receive traps, until their status is reset to *Active*. Select **Update** and press <**Enter**> to save changes.

Web-Based Management Configuration

The Management Capability Setup Menu allows enabling or disabling Web-Based Management and Out of Band Management. Use the space bar to toggle between settings. Select Save and press <**Enter** > to save the setting.

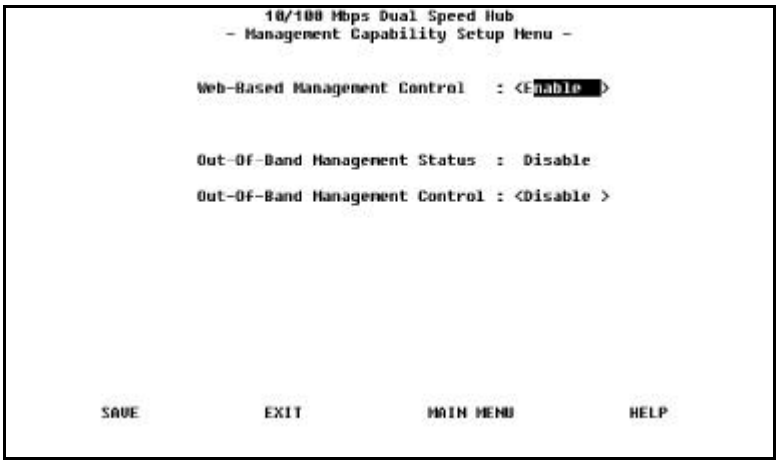


Figure 5.14 Management Capability Setup Menu

This menu lets you enable or disable Web-Based Management and Out-Of-Band Management.

Web-Based Management

You can enable or disable Web-based management. The new configuration take effect after executing **SAVE**.

Out-Of-Band Management Status

Displays the current status.

Out-Of-Band Management Control

You can enable or disable out of band management.

- When connecting with local console this setting takes effect immediately.

- When connecting with Telnet the system must be restarted before the setting takes effect.

Trap Filter

Selecting this option presents the Trap Filter Menu as shown in Figure 5.15.

10/100 Hub FHU-1201/1202/2401/2402TFXS
Trap Filter Menu -

(x) hubRfc1215LinkDownTrapFilter
(x) hubRfc1215LinkUpTrapFilter
(x) hubRfc1215AuthenticationTrapFilter
(x) hubRfc1516rptrHealthTrapFilter
(x) hubRfc1516rptrGroupChangeTrapFilter
(x) hubRfc1516rptrResetEventTrapFilter
(x) helloTrapFilter

***** Note *****

(x): the trap filter is turned-off and its associated trap is enabled.
( ): the trap filter is turned-on and its associated trap is disabled.

SAVE EXIT MAIN MENU HELP

Use <Tab> key to select the item, then press <Enter>

Figure 5.15 Trap Filter Menu

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

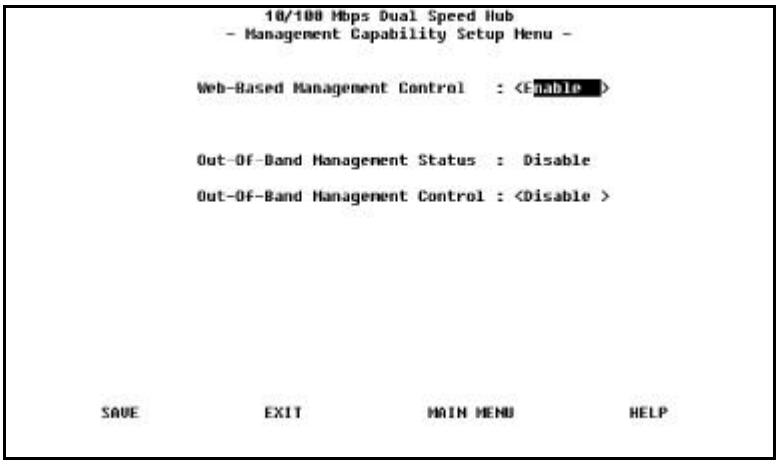


Figure 5.16 Web-Based Management Configuration

Controlling Devices

The Device Control Menu displays the configurable device sub menus.

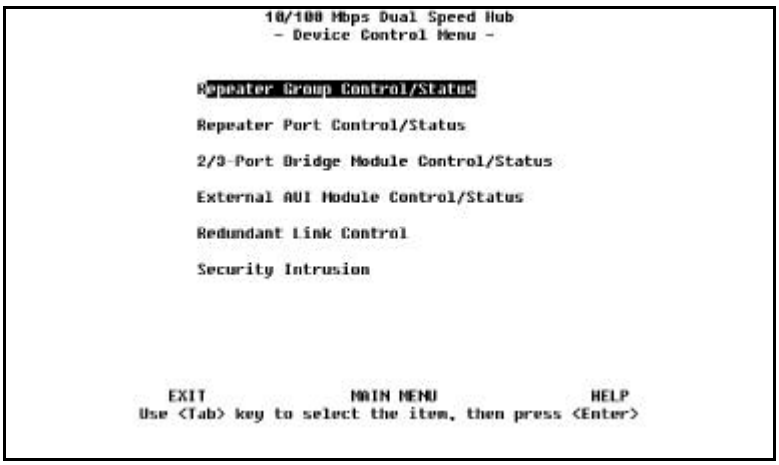


Figure 5.17 Device Control Menu

Repeater Group Control/Status

Allows you to read and configure all the hubs in a Hub FHU-1201/1202/2401/2402TFXS stack.

Repeater Port Control/Status

Allows you to read and configure ports on any hub in a Hub FHU-1201/1202/2401/2402TFXS stack.

2/3-Port Bridge Module Control/Status

Allows you to setup any Bridge (Switch) Modules such as Module MDU-0112TX, Module MDU-0113FX, Module MDU-0205TX, and Module MDU-0206FX in a Hub FHU-1201/1202/2401/2402TFXS stack.

External AUI Module Control/Status

Allows you to setup an AUI Module in a Hub FHU-1201/1202/2401/2402TFXS stack.

Redundant Link Control

Allows you to setup up to 24 redundant link pairs.

Security Intrusion

Allows you to setup Security.

Repeater Group Control/Status

The Repeater Group Control/Status displays status information for groups and allows enabling or disabling a group as well as naming and resetting the group.

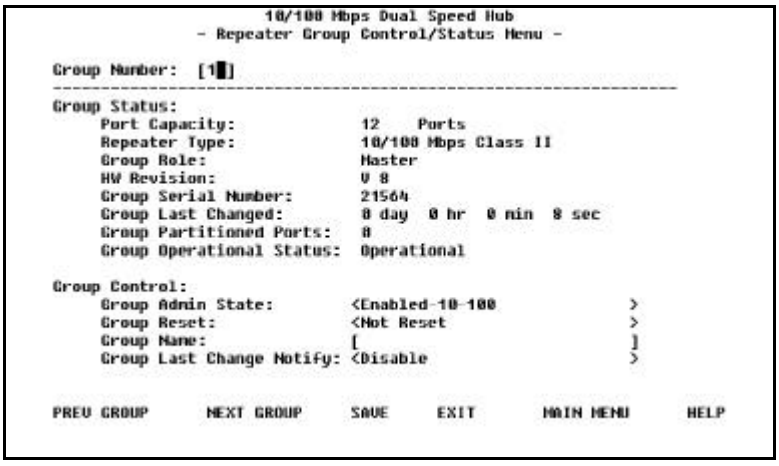


Figure 5.18 Repeater Group Control/Status

Group Number
The ID number of a hub in the stack, the range is 1~6.

Group Status

Port Capacity
The maximum number of ports that can be contained within the group (12/24).

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

Group Role
Describes the Hub's role as either master or slave.

HW Revision
The hardware version of the Hub FHU-1201/1202/2401/2402TFXS.

Group Serial Number
The serial number of the hub, for example 21564.

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

- hub cold or warm-started
- this instance of group was created (such as, when a device or module was added to the system)
- a change in the value of hub operational status
- ports were added or removed as members of the group (such as, group admin enabled or disabled)
- any of the counters associated with this hub that have been reset.

Group Partitioned Ports
The total number of partitioned ports in the group.

Group Operational Status
- Operational:
  The hub is connected to the stack.
- **Not Present:**
  The hub is not present.

Group Control

Lists the configurable functions and provides option fields, use Ctrl + S to toggle between options.

Group Admin State
Allows you to isolate one or both segments from the other hubs in a Hub FHU-1201/1202/2401/2402TFXS stack. When a segment is disabled, the segment cannot repeat to the other hubs the stack. The default value is Enabled 10 Mbps and 100 Mbps.

- **Enable-10 –100 (Default)**

Both 10 Mbps and 100 Mbps segments of a given hub are connected to the back plane of stack. This is the default.

- **Disable 10-100**
  Both 10 Mbps and 100 Mbps segments of the hub are isolated from stack.
- **Enable 10**
  Only the 10 Mbps segment of a given group is connected to the back plane of stack. The 100 Mbps segment of a given group is isolated from stack
- **Enable 100**
  Only the 100 Mbps segment of a given group is connected to the back plane of stack. The 10 Mbps segment of a given group is isolated from stack

Group Reset

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

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

- **No Reset**
  None of these are 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'. That 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.

Group Last Change Notify

- **Enable**
  Sends out a trap when the value of this field changes.
- **Disable**
  Does not send out a trap when the value of this field changes.

To change the setting of a given group:

1. Select the group by number.
2. Set new value to Group Admin State.
3. Set reset request to Group Reset field.
4. Type in the name to the Group Name field.
5. Set Group Last Change Notify field.
6. Select **SAV**E.

Repeater Port Control/Status

The Repeater Port Control/Status displays status information for each port, of each linked repeater, and allows enabling/disabling, setting the speed, and enabling/disabling link status change notification for ports.

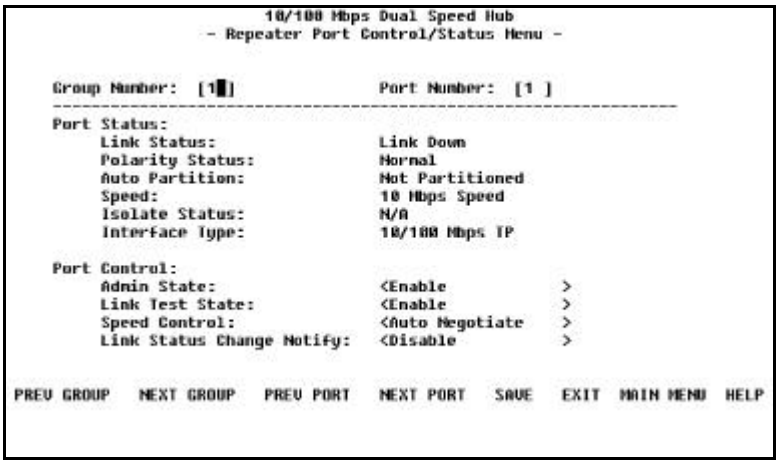


Figure 5.19 Repeater Port Control/Status

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

Group Number

The Hub FHU-1202/2402TFXS ID assigned to the hub in the stack. (1 to 6)

Port Number

The port number (1~24)of the hub specified in the Group Number.

Port Status

Displays the current read only settings.

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 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.

- **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 repeater.

Auto Partition

The current partition status of the port.

- **Not Auto Partitioned**
  The port is not partitioned
- **Auto Partitioned**
  The port is partitioned

Speed

This is the current speed of this port. The default is Auto Negotiate.

- **Auto Negotiate**
  The port speed is automatically negotiated with the device connected to the port to the fastest speed.
- **Force 10-TP**
  The port is forced to operate at 10 Mbps only, and can only pass data with 10 Mbps devices.
- **Force 100 TP**
  The port is forced to operate at 100 Mbps only, and can only pass data with 100 Mbps devices.

Isolate Status (100Mbps Port Only)

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

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

Port Control

Lists the configurable functions and provides option fields, use Ctrl + S to toggle between options.

Interface Type

The interface type of the port. (TP port interface type)

Admin State

The current administration state of the port. (enable/disable)

Link Test

Enable or disable link testing.

Speed Control

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

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

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 hub.

2/3-Port Bridge Module Control/Status

This menu displays settings and allows configuring of a bridge (switch) module in a given hub in the stack.

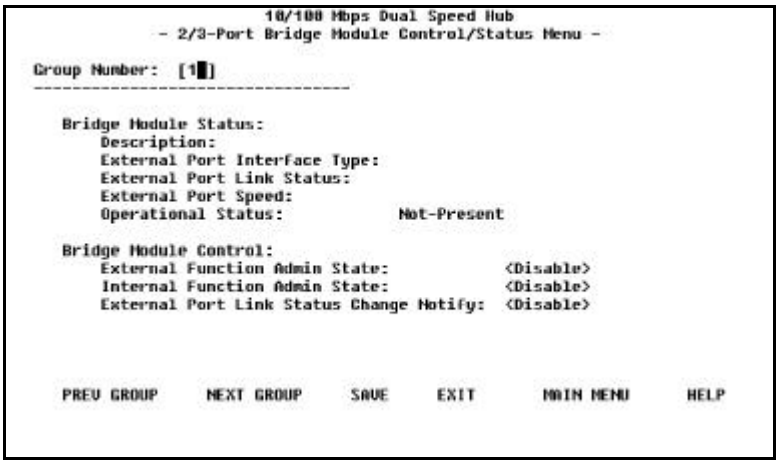


Figure 5.20 2-Port Switch Module Control/Status Menu

Group Number

The hub ID number assigned to the Hub FHU-1202/2402TFXS. (1 to 6)

Bridge Module Status

Displays the current read only settings

Bridge Description

A description of the characteristics of this bridge module.

- **MDU-0112TX Bridge or 10/100BASE-TX Distance Extender**
- **MDU-0205TX Bridge and 10/100BASE-TX Distance Extender**
- **MDU-0113FX Bridge or 100 BASE-FX Distance Extender**
- **MDU-0206FX Bridge and 100 BASE-FX Distance Extender**

External Port Interface Type

Indicates the interface type of external port for a given 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. Read only

- **Link Up**
- **Link Down**

External Port Speed

The modules external port speed. Read only.

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

Hardware Status

Indicates the operation status of this module.

- **Operate as Internal Plus External Bridge**
  The internal bridge function and the external distance extender 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

Lists the configurable functions and provides option fields, use Ctrl + S to toggle between options.

External Function Admin State

The default value is Disable.

- **Enable**
  Enables the external bridge function.
- **Disable**
  Disabled external distance extender function of a given module. Once the distance extender function is disabled, you must enabled it, to restore external distance extender operation.

Internal Function Admin State

The default value is Disable.

- **Enable**
  Enables the internal bridge function. The internal hardware Jumper switch must also be enabled for the internal bridge to function.

Note: The internal bridge must be enabled in hardware with the Jumper switch settings before the Admin state can be enabled.

- **Disable**
  Disables the internal bridge function. Once the internal bridge function is disabled, the you must enabled it, to restore internal bridge operation.

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

External Port Link Status Change Notify

When 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.

Redundant Link Control

The Redundant Link Control menu allows configuring up to 24 pairs of redundant links. A redundant pair consists of any two physically linked ports in the Hub FHU-1202/2402TFXS 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. In the event that 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.

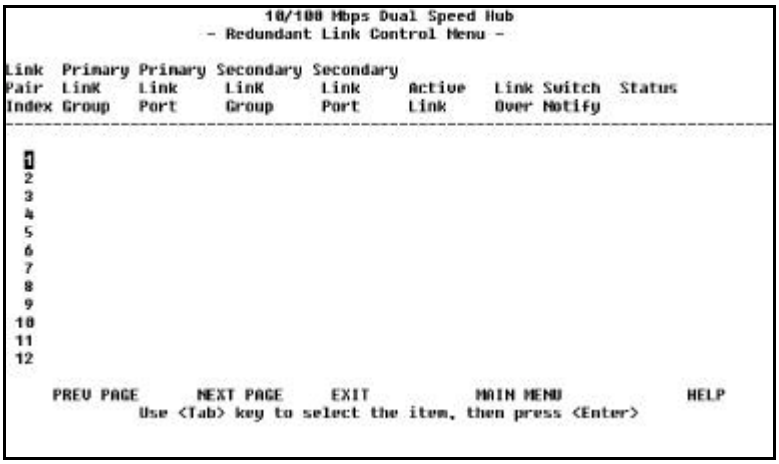


Figure 5.21 Redundant Link Control

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 24)

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

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

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

Secondary Link Port
This object identifies the port number of 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 active primary link.
- **Secondary**
  The port is currently the secondary port.
- **Both fail**
  Both the primary and the secondary have failed.

Link Switch Over Notify
If the link status of active link is *down* for more than five seconds then the *active link failed* is detected and "port switch over" is performed and a trap is sent to the trap receivers.

- **Enable**
  A trap is sent to the trap receivers if a switch over occurs.
- **Disable**
  No trap is sent to the trap receivers if a switch over 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, the status of this link pair is changed to the *suspend state* and indicates that 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 on, the status of this link pair is changed to enabled and the redundant link pair is in the normal operation mode.

Note: Setting the redundant link to disable does not cause the ports to be switched over.

- **Suspend**
  Indicates that the active ports are disabled and the redundant link function is temporary suspended until you set its state to *enable*.

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** re-assigns 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.

Configuring Link Pairs

1. Select a Link Pair. (1-24) Use NEXT PAGE to select pairs 13 through 24.
2. Enter the Primary Link Group (1 to 6).
3. Enter the Primary Link Port (1 to 12/24)
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.
5. Enter the Secondary Link Port. (1 to 12/24)
6. Enable the Link Switch Over Notify. (Optional)
7. Enable the Status.
8. Select **Save** to update the new Linked Pair. Repeat these steps for each Link Pair.

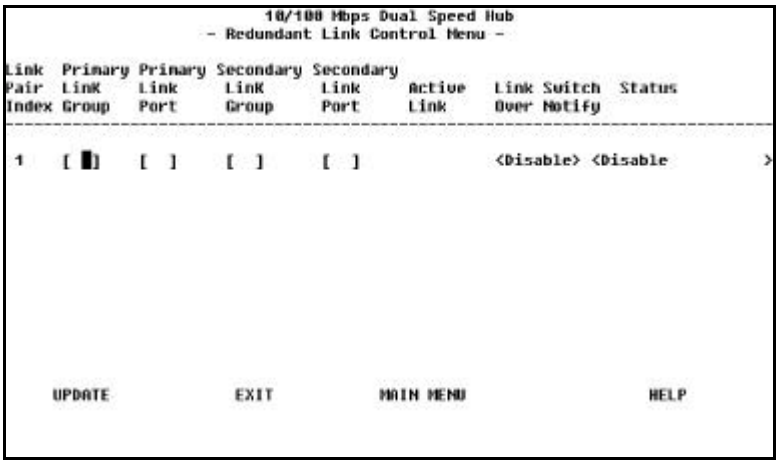


Figure 5.22 Configuring Redundant Link Control

Editing a Link Pair

You can edit a Link Pair by entering the Link Pair number (of an existing Link Pair) and reconfigure the rest of the columns, then select **Save**, the Link Pair is updated to the new settings.

Deleting a Link Pair

You can delete a Link Pair by entering the Link Pair number (of an existing Link Pair) and setting the Status to Invalid, then select <**Save**>, the Link Pair is removed.

Security Intrusion

The Security Intrusion Control/Status Menu allows setting up security features.

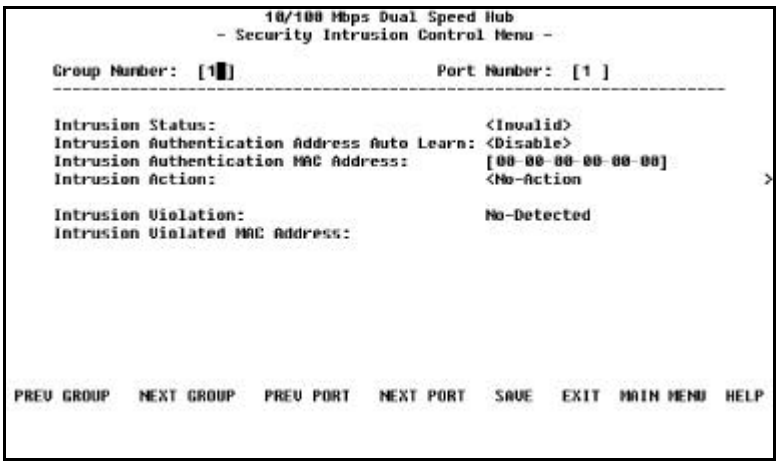


Figure 5.23 Security Intrusion Control/Status Menu

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 Hub FHU-1201/1202/ 2401/2402TFXS. (1-6)

Port Number

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

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.
- **Disabled**
  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 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.

- **Both**
  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.

Note: 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.

Monitoring Network

Statistic counters can be monitored for each repeater group and its ports. The Monitoring Network Menu displays the monitoring sub menus.

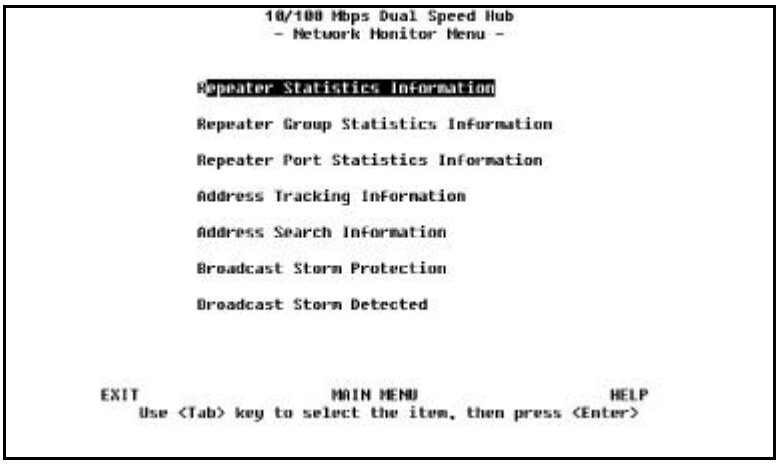


Figure 5.24 Monitoring Network Menu

Repeater Statistics Information

Hub statistics such as Tx collisions, total frames and total errors and total octets for both 10 Mbps segment and 100 Mbps segment.

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

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

Monitor 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 presents the Repeater Statistics Information Menu as shown in Figure 5.24.

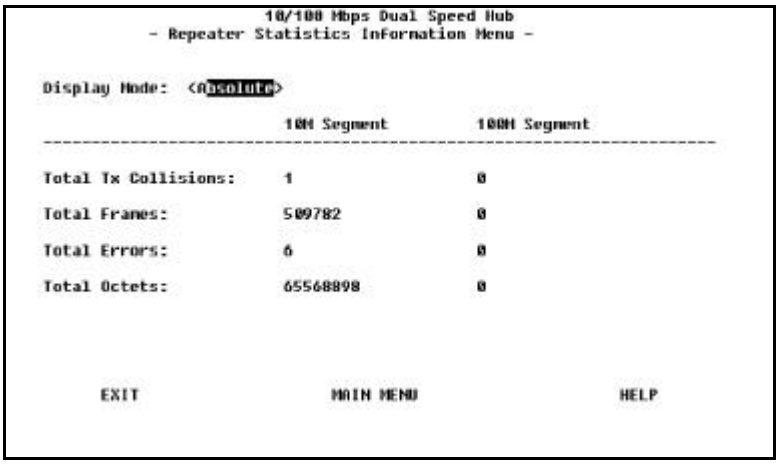


Figure 5.25 Repeater Statistics Information Menu (Absolute)

You can monitor the statistics in Absolute or Relative counters. The default is Absolute counters.

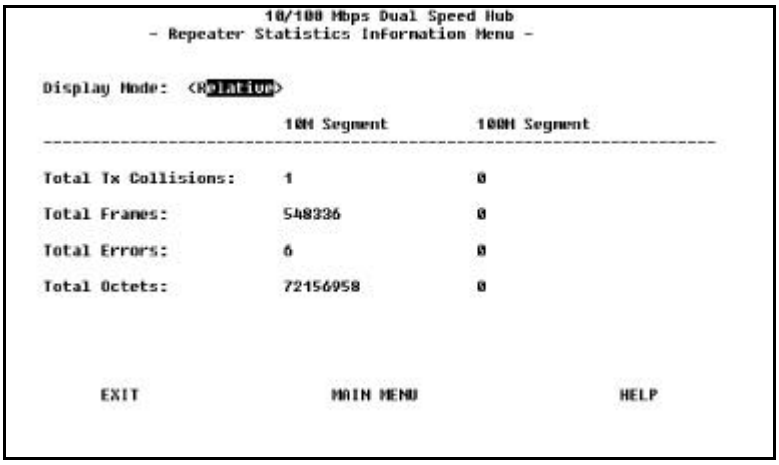


Figure 5.26 Repeater Statistics Information Menu (Relative)

Total Tx Collisions
The number of transmission collisions that have occurred in this hub.

Total Frames
The number of frames received in this hub.

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 Mismatches.

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

Repeater Group Statistics Information

The Repeater Group Statistics Information Menu displays statistic counter for each group.

Absolute

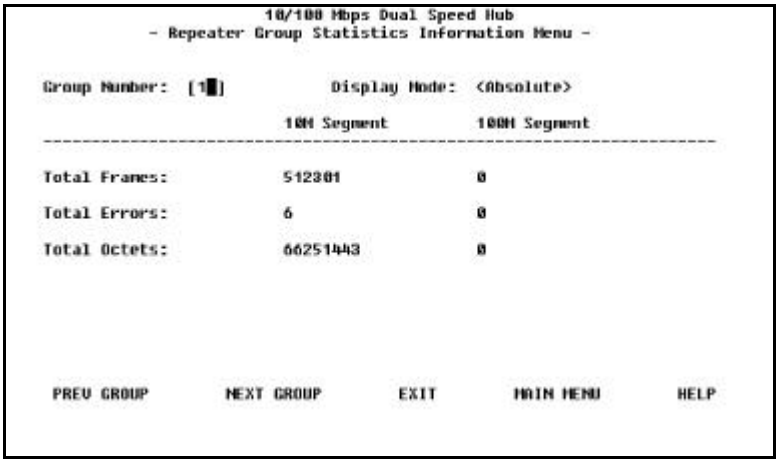


Figure 5.27 Repeater Group Statistics Information Menu (Absolute)

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 start. You can not clear absolute counters using the CLRCNT. Absolute counters are reset by either Group Reset-All or Group Reset Counters only. 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 then changing back to Relative Mode.

Relative

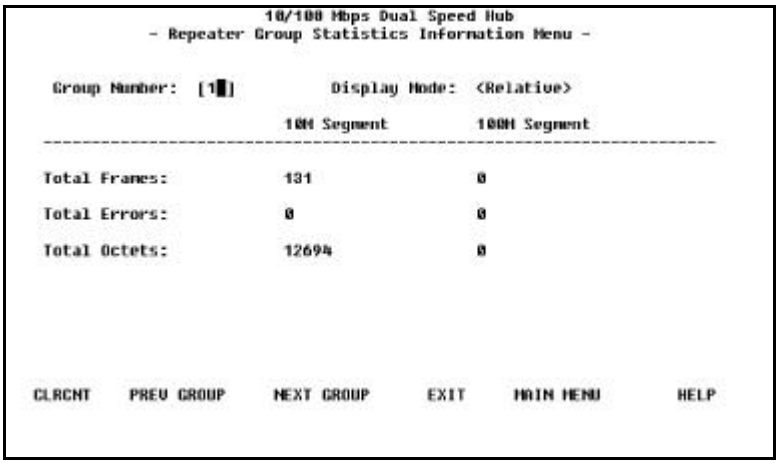


Figure 5.28 Repeater Group Statistics Information Menu (Relative)

Total Frames
The number of frames of valid frame length that have been received on the ports of this hub and not including FCS Error and Collision Event.

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

Tx Collisions
The total number of transmission collisions on this hub.

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.

Repeater Port Statistics Information

The Repeater Port Statistics Information Menu shows statistic in *Absolute* and *Relative* values.

Absolute

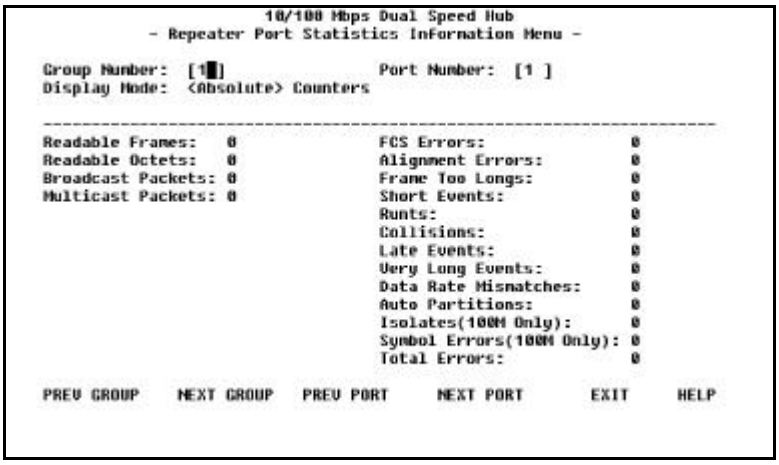


Figure 5.29 Repeater Port Statistics Information Menu (Absolute)

The Repeater Port Statistics Information Menu displays counter information for the current port of the current hub. A hub can be selected with the PRE GROUP and NEXT GROUP commands and its ports with the PRE PORT and NEXT PORT commands.

Relative

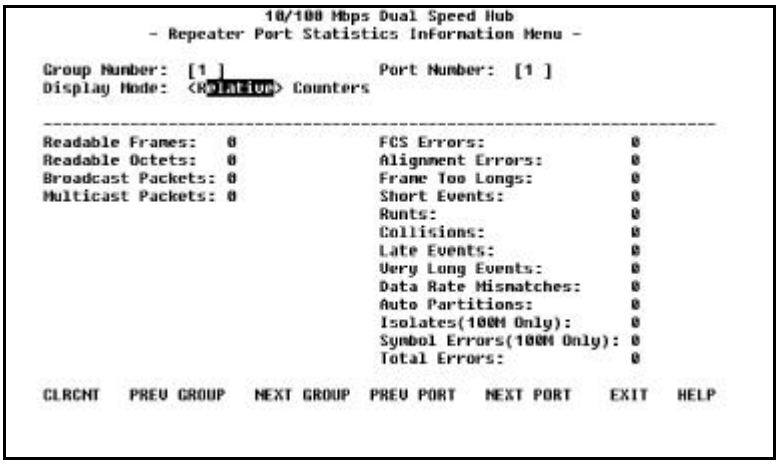


Figure 5.30 Repeater Port Statistics Information Menu (Relative)

Display Mode
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 Hub FHU-1202/2402TFXS in the stack. (1 to 6)

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

Display Mode
Display counters in Absolute or Relative values.

Readable Frames
Total readable frames received by the port.

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

Multicast Packets
The total number of good packets received which 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 Sequence.

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 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 activity duration was 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.

Data Rate Mismatches
Total frames received by the port with no collisions and the activity duration was greater than the ValidPacketMinTime event and also

frequency (data rate) is detectably mismatched from the local frames mismatch frequency.

Auto Partitions
Total number of times the port was auto-partitioned.

Isolates (100 Mbps 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 which 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 (100 Mbps 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. 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

The Address Tracking Information Menu provides per port based, node tracking capability (MAC address based). This capability provides the basic traffic analysis capability to diagnose network problems, such as *Intrusion*. The node tracking function records the source MAC of each data packet and provides the filters for data analysis.

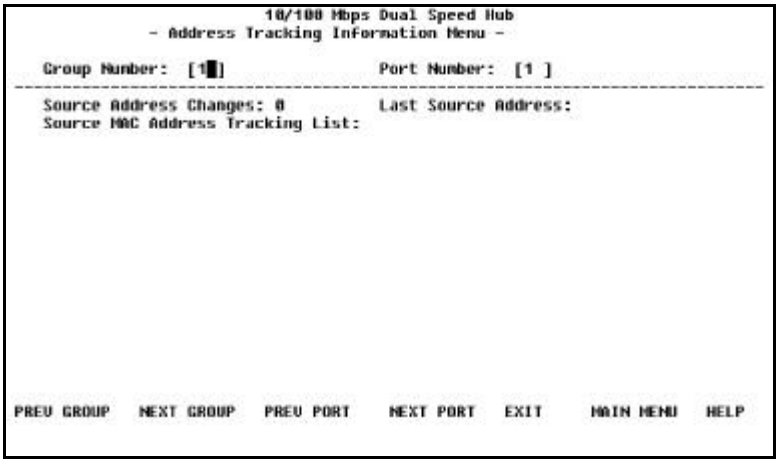


Figure 5.31 Address Tracking Menu

Source Address Changes

This counter is incremented by one for each time that the Last Source Address for this port has changed. 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-E0-95-00-00-00 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 list does not age out, the first entries are deleted to accommodate new entries when the list is full.

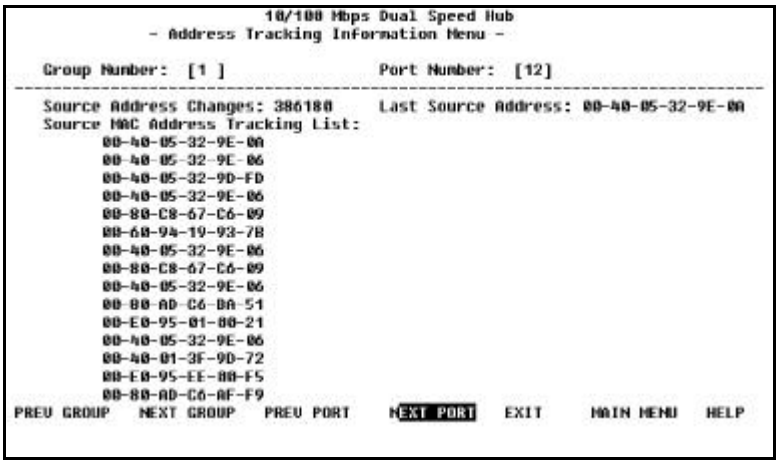


Figure 5.32 Address Tracking Information Menu (list)

Address Search Information

Selecting this option presents the Address Search Information Menu as shown in Figure 5.33.

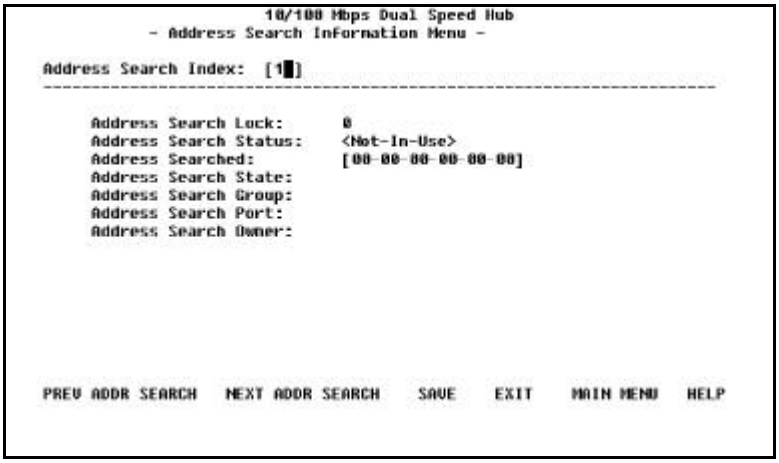


Figure 5.33 Address Search Information Menu

The Hub FHU-1201/1202/2401/2402TFXS provides per segment based source (MAC address) matching capability. 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 source address to be searched in the system for which this entry contains information. (1-8)

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 Integer Type and then role 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 to 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 does not detect the address of any port.

Address Search Group

The group number received, whose source address corresponds to the address searched.

Address Search Port

The port number received, whose source address corresponds to the address searched.

Address Search Owner

The entity which currently has *ownership* of this search entry

Broadcast Storm Protection

The Hub periodically monitors the broadcast counters of each hub port to detect a broadcast storm condition. If a hub port is detected to be causing broadcast storm it is automatically partitioned, and a trap is sent to the network manager. The Hub continually monitors those ports that have been partitioned to check if the broadcast storm condition still exists. The partitioned hub port is auto recovered to normal operation once the broadcast storm condition is released.

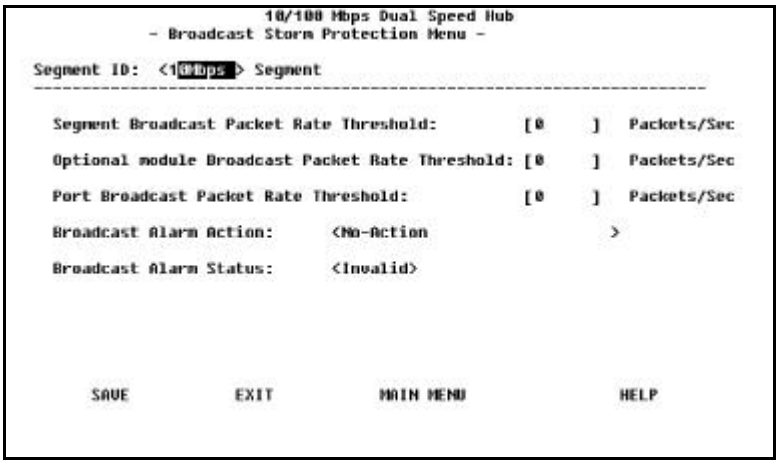


Figure 5.34 Broadcast Storm Protection Menu

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

The 10 Mbps segment or the 100 Mbps segment.

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 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, the Alarm Detection Status will be set to *Detected*, and the proper 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 broadcast storm, the Broadcast Storm protection function will continue to monitor the port based on the following rule:
  a) The port is disabled for 15 seconds, enabled again for 5 seconds.
  b) If the storm exists for 2 minutes the port is disabled and not monitored.
  c) If the broadcast storm still exists, a and b are repeated.

Note: It is up to the user to enable the port once the source of the broadcast storm has been handled..

- **Send Trap and Partition**
  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

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

Broadcast Storm Detected

This menu displays a list of ports that Broadcast Storm has been detected on.

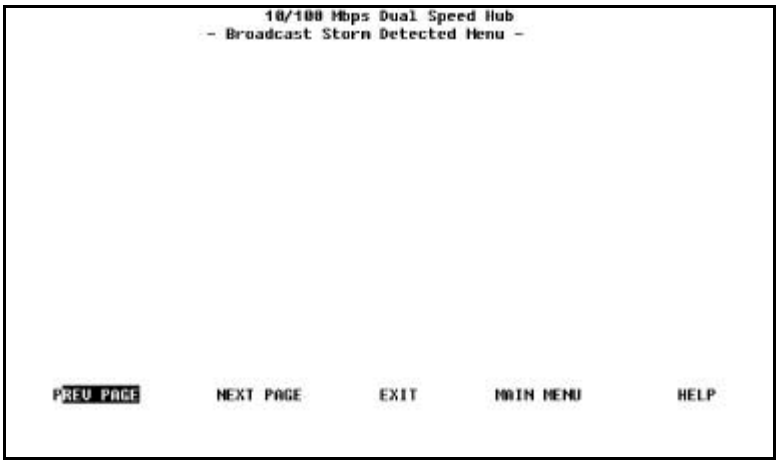


Figure 5.35 Broadcast Storm Detected Menu

Each broadcast storm is detected, the hub and port number is listed in this menu. If there has been no storms 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

The User Authentication Menu is used to assign user login names, passwords and read/write privileges. The Mini-Console password can be configured in the User Authentication Menu.

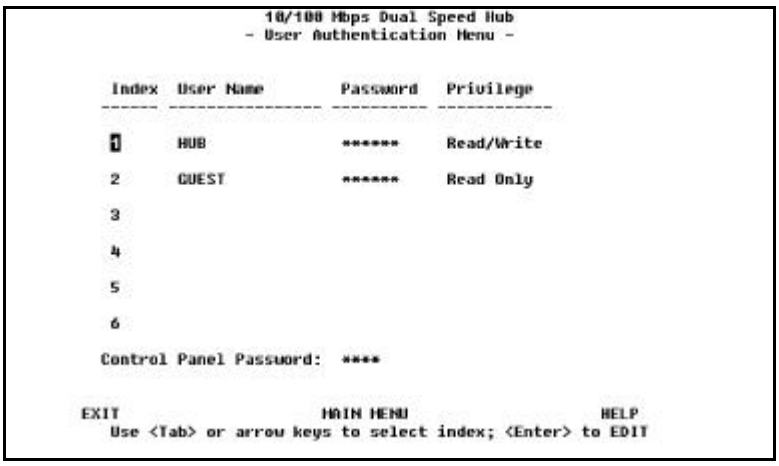


Figure 5.36 User Authentication Menu

To define each user authentication select an index number and press **Enter**.

Use the ADD command to add a name. A user name and password can be deleted using the DELETE command. Select the EXIT command to return to the previous screen and view the results.

Note: You can configure the user Authentication information (password) of the Mini-Console with Local Console or Remote Telnet. The factory default Mini-Console password is “0000”.

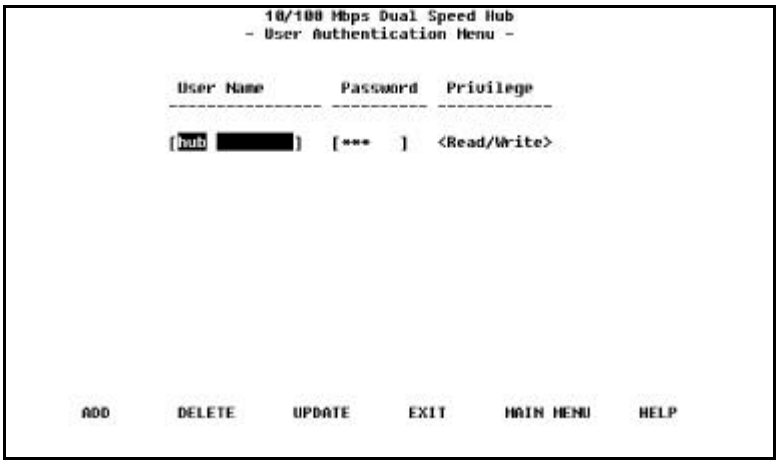


Figure 5.37 User Authentication Menu (editable)

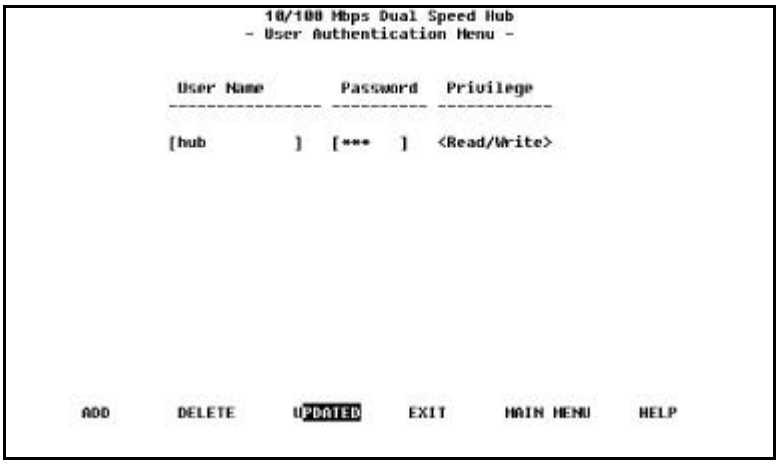


Figure 5.38 User Authentication Menu (updated)

Select the index number first and press <**Enter**>. Enter a user name of up to 12 characters and password of up to 6 characters, specify read/write privilege and then press **Enter**.

System Utility

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

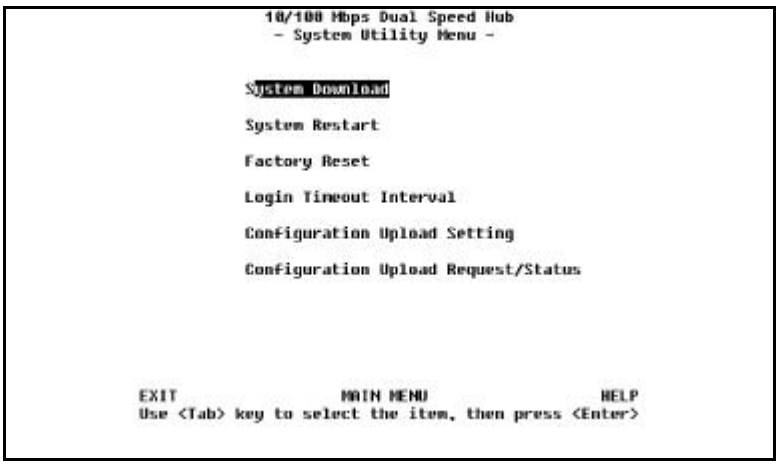


Figure 5.39 System Utility Menu

System Download
System downloads are used to update system software or replace existing software that has become corrupted.

System Restart
The system can be restarted at any time and is required after certain configuration settings are made.

Factory Reset
The system can be reset to the original settings, however all custom settings will be lost.

Login Timeout Interval
Set the amount of time before a Telnet automatically logs out, when requesting an upload.

Configuration Upload Setting

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

Configuration Upload Request

Submit a request for a configuration file upload.

System Download

The System Download Menu enables reading Boot Sever Information from a remote BOOTP Server and to down load system configuration files, Web Server database information and system software from a remote TFTP Server. To download software check **Bootp Request**, select the appropriate download function, enter the filename with the full path, save the configuration and finally restart the device from the System Restart Menu.

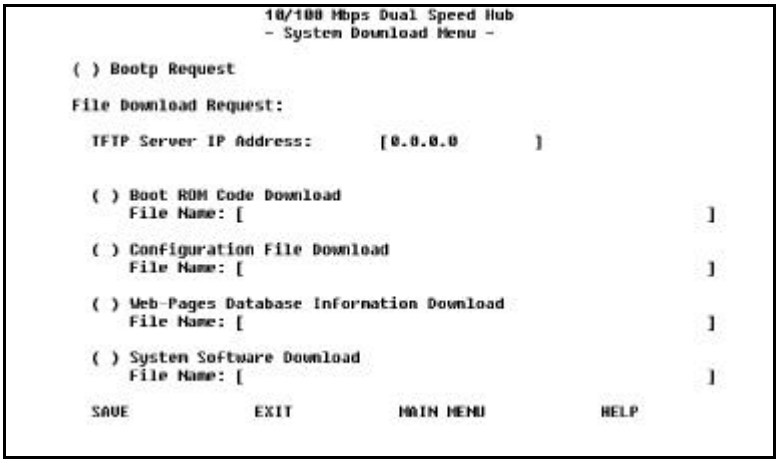


Figure 5.40 System Download Menu

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:

1. Select Bootp request

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

2. Perform a cold restart on the system.

   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.

   Note: Use the following naming convention:

   - **Boot ROM Code download - 110Vxxx.BT**
   - **Web Pages Database Information Download – 110Vxxx.WEB**
   - **System Software Download - 110Vxxx.RT**
     where, xxx is the version number.

To download TFTP code, perform the following:

1. Enter the IP address of the TFTP server.
2. Select the downloads that you want to perform.
3. Enter the path and file name for each of the downloads you have selected (for example, C:\microcode\110V101.BT).
4. Save the configuration.
5. Restart the system.

System Restart

The System Reset Menu allows the user to reset the system with a **Cold** or **Warm** reset.

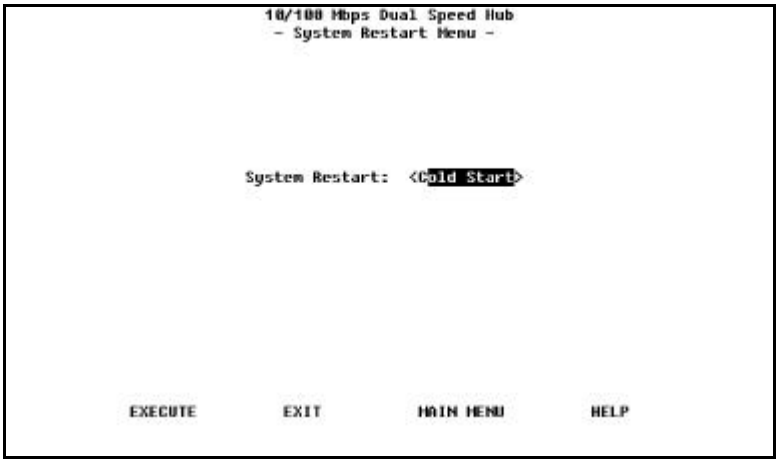


Figure 5.41 System Restart Menu

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 select **Enter**, a warning message informs the user that system restart will be performed right now.

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 BOOTROM level and is the same as unplugging and re-plugging power to the hub. A cold restart is needed when the user performs a BootP request or code download.

Factory Reset

The Factory Reset Menu allows resetting Hub FHU-1202/2402TFXS to the original factory settings. All user configurations will be lost. A "*confirm"* messages is displayed before the hub is reset, the user can abort the factory reset.

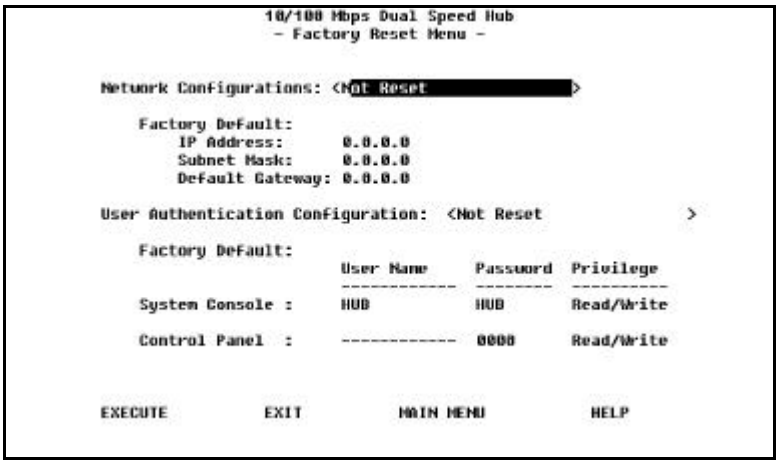


Figure 5.42 Factory Reset Menu

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, do the following steps:

1. Select how the user wants network configuration processed during a factory reset:
   - **Not Reset**
     Current 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.

2. Select how the user wants the user authentication configuration 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.
3. Select EXCUTE and press Enter.

When EXECUTE and **Enter** are selected, a warning message inform the user that system configuration data will be reset right now.

Login Timeout Interval

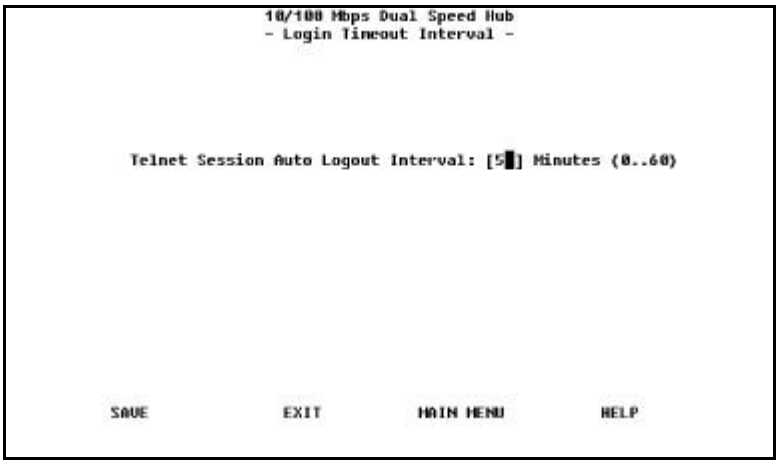


Figure 5.43 Login Timeout Interval Menu

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

Configuration Upload Setting

Hub FHU-1202/2402TFXS provides the capability to upload the hub configuration data to the remote server in binary format. You can upload your configuration files and save as a backup in case you need to restore your system settings if necessary.

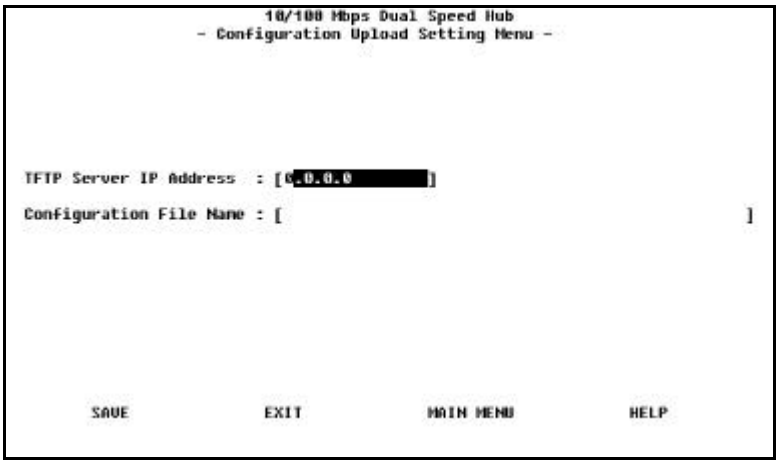


Figure 5.44 Configuration Upload Setting Menu

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 on 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 4-49.

TFTP Server IP Address:

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

Configuration File Name:

The name of the configuration file and the full path.

Configuration Upload Request

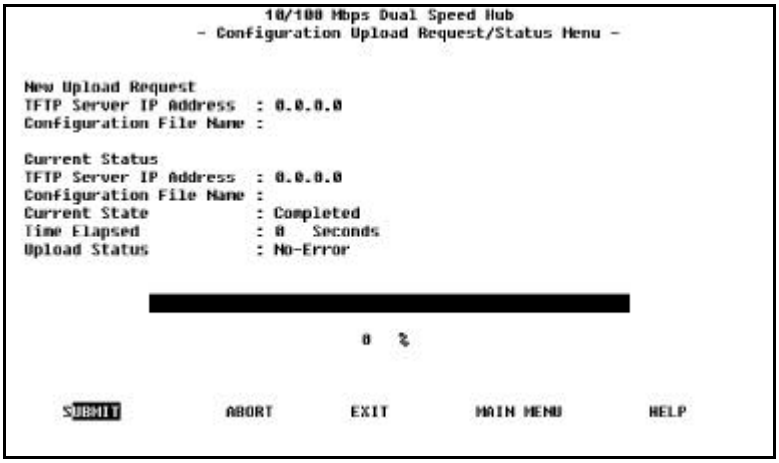


Figure 5.45 Configuration Upload Request

This menu enables you to submit a request for a configuration file upload and view the status of a download. Select SUBMIT to make the Upload Request.

TFTP Server IP Address

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

Configuration File Name

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, can not be found on the TFTP Server.
- **Access Violation**
  The file specified Configuration Filename field is Write Protected.
- **Disk Full**
  The disk specified Configuration Filename field, is full.
- **Timeout**
  The TFTP upload timeouts has expired, 20 seconds. A progress bar is displayed in the menu showing the progress.
- **Other**
  Other errors that are defined by the system.

Once you have uploaded your configuration files you can download them if necessary. See “System Utility” on page 5-8, for information about downloading configuration files.

Chapter 6

SNMP Management (For Hub FHU-1202/ 2402TFXS Only)

Managing via MIB File

Hub FHU-1202/2402TFXS's built in Management Information Base allows it to be managed by any MIB file browser. For more detailed information on SNMP management see the Hub FHU-1202/2402TFXS software manual.

Managing through HP-OpenView

HP-Openview is an advanced SNMP management program that can be used to manage Hub FHU-1202/2402TFXS. HP-Openview is designed to manage large network or campus networks and Hub FHU-1202/2402TFXS is designed to meet work together in those environments. Hub FHU-1202/ 2402TFXS comes complete with a special HP-Openview management module (on diskette) with a GUI interface similar to a Web-Browser.

Appendix A

Product Specifications

Standards Compliance
IEEE 802.3 10BASE-T, 10BASE5 Ethernet
IEEE 802.3u 100BASED-TX Ethernet

Number of Ports
12 / 24 auto-sensing 10 / 100M Ethernet (RJ-45) ports

Display Panel
For Hub FHU-1202/2402TFXS Master:
Vacuum Fluorescent Display (VFD) providing extensive network status information including utilization graphs and statistics at a glance
For Hub FHU-1201/2401TFXS:
Rich diagnostic LEDs indication
Link / Rx per port
Forwarding indicator for both 10 / 100Mbps segments
Collision indicator for both 10 / 100Mbps segment
10 / 100Mbps indicators with internal / external switch module activities

Media Interface Exchange
2 10 / 100Mbps Uplink ports (MDI-II) shared with port 1 & port 12 respectively

Stacking
6 hubs per stack
SCSI daisy-chain
Automatic Unit ID numbering
Management data on serial daisy-chain
Class II repeater

Expansion Slot
1 slot for network management unit (only FHU-1202 / 2402TFXS Master)
1 slot for optional switch module

Smart Mini-Console Display on FHU-1202/2402TFXS Master
Configuration, device / port management, and network statistics monitoring
Three keys on the front panel to perform for all the Mini-Console functions
VFD (Vacuum Fluorescent Display) panel displays text & graphic information

Key Management Features (thru Web and SNMP)
Master / Slave management architecture
Per port address tracking
Per stack source address search capability
Network traffic monitoring
Duplicated IP detection
Intrusion control per port security
24 pairs of redundant link
Broadcast storm protection
BOOTP/TFTP software download supported
Console/Telnet Management
VT-100 terminal interface supported
Local console management via RD-232 (DB-9) port

In-band/out-of-band remote telnet management

Web-Based Management

Complete web server embedded in device
Integrated HTML forms and Java™ applets
Standard web server security to total network protection
Photographic quality GUI to configure / monitor
Management from anywhere and any platform

SNMP Management

Supporting standard RFC 1213 MIB II, RFC 1516 Repeater MIB, and proprietary MIBs
Supporting RFC 1757 RMON Group 1, 2, 3, and 9
In-band / Out-of-band management
Device managers for HP-OpenView

Power Requirements

100 - 240 VAC, 50 / 60 Hz
Internal universal power supply

Environment

Operating Temperature: 10° to 40°C
Storage Temperature: -25° to 70°C
Operating Humidity: 8% to 80% non-condensing

Safety Regulations

CUL (UL & CSA)
LVD

EMI Certifications

CE Mark
FCC Class A
VCCI Class 1

Dimensions

W x D x H : 440 x 221 x 56.5 mm

Weight

2.85 kg

Mounting

Standard EIA 19″ rack mount

Ordering Information

Stack Hub FHU-1202/2402TFXS
12/24 ports auto-sensing 10/100Mbps Master Hub with Local console/Remote Telnet management, SNMP, Web-Based Management & Mini-Console Management

Stack Hub FHU-1201/2401TFXS
12/24 ports auto-sensing 10/100Mbps Slave Hub

Optional Module:

Module MDU-0112TX
Bridge **or** 10/100BASE-TX Distance Extender Switch Module (MDI-X and MDI-II interface)

Module MDU-0113FX
Bridge **or** 10/100BASE-FX Distance Extender Switch Module (SC-type connector)

Module MDU-0205TX
Bridge **and** 10/100BASE-TX Distance Extender Switch Module (MDI-X and MDI-II interface)

Module MDU-0206FX
Bridge **and** 10/100BASE-FX Distance Extender Switch Module (SC-type connector)

Module 10AUI
10BASE-5 AUI Switch Module

SNMP Network Management:
Manager FHU-1202/2402TFXS
Hub FHU-1202/2402TFXS Device Manager for OpenView/NT

Appendix B

Error Messages

Appendix C

Mini-Console Menu Tree

Appendix D

Troubleshooting Network Looping

Q: The local-console 'login screen' does not come up sometimes when a terminal (PC running terminal emulation) is connected to already booted FHU-1202/2402TFXS master hub. Why?

A: The screen must be refreshed, when Hub FHU-1202/2402TFXS is running and the terminal emulator is started. Pressing Ctrl + R refreshes the screen and the login menu appears.

Q: Users of the 100Mbps segment cannot use Web Management, however 10 Mbps segment users can. Why?

A: The SNMP agent, TCP/IP stack and the Web engine are implemented on the 10 Mbps bus of the master hub. Therefore the 10 Mbps segment should be used for Web Management in the absence of a switch module.

Q: Even though the switch module with internal bridging has been installed, the 10 Mbps segments can't communicate with the 100 Mbps segments. Why?

A: The switching function is disabled by default in the software, therefore even though the internal function is enabled with the on board jumpers, 10 Mbps and 100 Mbps segments cannot communicate. The internal switch must be enabled using local console management through a connections from the RS232 port on the hub to a serial port on a PC. Select Device Control

from the main menu and then 2/3 port bridge module control/status. Enable the internal switch.

Q: With regards to Hub FHU-1201/1202/2401/2402TFXS modules: Users will need to use Web or Console management to enable the module, however, what if users only have a FHU-1201/2401TFXS model in their LAN and want to install a MDU-0112TX as an internal switch or have a MDU-0205TX as both internal and external, or have another FHU-1201/2401TFXS model in the stack and one MDU-0112TX as an external switching port?

A: In the case of FHU-1201/2401TFXS (whether single or multiple stacked), the switch module would function straightaway when installed. The mode ("internal" or /and "external) can be set on the module PCB using the jumpers provided. When the master hub is present, we need to additionally enable the module's function in the management software (through Local Console or Web/SNMP)

Q: Is there loop detection and isolation feature available in Hub FHU-1201/1202/2401/2402TFXS, in case two switch modules (internal bridging enabled on the hardware) are installed in the same stack.

A: No. The stack will get into a loop even before the software has booted. Therefore, the only control is on hardware (jumpers on the PC board)

Appendix E

Index