SuperStack II Hub 10 Management User Guide

Management Module (3C16630A)

Advanced RMON Module (3C16632)

Part No. DUA1663-0BAA03
Revision: 01
Published September 1996

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145

3Com Ireland reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Ireland to provide notification of such revision or change.

3Com Ireland provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:

Restricted Rights Legend: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for restricted Rights in Technical Data and Computer Software clause at 48 C.F.R. 52.227-7013.
3Com Ireland c/o 3Com Limited, ISOLAN HOUSE, Brindley Way, Hemel Hempstead, Herts. HP3 9XJ. UK.

For civilian agencies:

Restricted Rights Legend: Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

3Com, CardFacts, NetFacts, **CardBoard** and **Transcend** are registered trademarks of 3Com Corporation. Registered trademarks are registered in the United States, and may or may not be registered in other countries.

SuperStack and **SmartAgent** are trademarks of **3Com Corporation**.

3ComFacts and **Ask3Com** are service marks of **3Com Corporation**.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

The technology behind **3Com's LAN Security Architecture** is protected by U.S. patents 5161192 and 5386470 (foreign patents pending).

CompuServe is a registered trademark of CompuServe, Inc. [List any other company trademarks here.]

Other brand and product names may be registered trademarks or trademarks of their respective holders.

CONTENTS

ABOUT THIS GUIDE

1 INTRODUCTION

2 INSTALLATION AND SETUP FOR MANAGEMENT

3 USING THE VT100 MANAGEMENT INTERFACE

A TECHNICAL INFORMATION, CABLE PIN-OUTS AND PROTOCOLS

B TECHNICAL SUPPORT

ABOUT THIS GUIDE

A Word about Safety

Please pay careful attention to the Warning and Safety Information panels that appear throughout this guide. These panels give information that will protect YOU and the SuperStack II equipment.

Look for the Warning symbol, ⚠

which always accompanies the appropriate message.

⚠ **WARNING:** *Installation and Removal of the SuperStack II Hub 10 Management Module or Advanced RMON Module must only be carried out by Qualified Personnel.*

About this User Guide

This guide describes how to install the SuperStack II Hub 10 Management Module and SuperStack II Hub 10 Advanced RMON Module and use them to manage SuperStack II stacks via the VT100 interface or an SNMP application. A stack is one or more units (such as SuperStack II Hub 10 12 Port TP) which you connect together to function and manage as a single logical repeater.

Throughout this guide, Module can be taken to refer to either product.

The guide is written for the system or network administrator who is responsible for setting up devices used on the network. If you are using management on your network for the first time it is possible you will make mistakes. We have tried to identify the likely errors you may make and have provided hints and tips to help you recover from error situations. If you are already familiar with network management you will be able to skip some of the information in the guide and use the information given for reference purposes.

The guide assumes that you are familiar with VT100 terminals, modems, PCs and SNMP. You will need to refer to other manuals for this information. See "Other Useful Publications" on page ix.

This guide explains:

- How to install the Module.
- How to set up and use the management facility which is provided by the module, in order to manage a stack.
- How to access the facility locally using a VT100 terminal or a PC using terminal emulation software.
- How to access the facility remotely using a modem and a VT100 terminal or a PC using terminal emulation software.
- How to access the facility remotely over a TCP/IP network using Telnet.
- How to access the facility locally or remotely from a workstation running SLIP, using Telnet or SNMP management.

This guide does *not*:

- Show you how to install SuperStack II Hub 10 units.
- Explain how to manage units using an SNMP Manager such as Transcend WorkGroup Manager for Windows.
- Provide a detailed description or copy of the MIB (Management Information Base). You can obtain a copy of the MIB from 3Com's bulletin board services if required. For more information, see Appendix B.
- Show you how to use your Telnet host application.

If the information in the release notes shipped with your product differs from the information in this guide, follow the release notes.

How to Use This Guide

The following list shows where to find specific information.

If you are looking for:	Turn to:
An overview of the features of the Modules and how to make best use of them. Also, details of compatibility with LinkBuilder FMS, FMS II, 10BT and 10BTi.	Chapter 1
Details of how to install the Module into your SuperStack II Hub 10.	Chapter 2
Information about how to use the VT100 interface to manage your SuperStack II Hub 10 stack.	Chapter 3
Technical information and cable pin-outs.	Appendix A
Information about obtaining technical support and 3Com repair services.	Appendix B
Troubleshooting information.	Appendix C
Information about interpreting statistics.	Appendix D
Information about RMON Support.	Appendix E
Index of management action and data.	Appendix F

Other Useful Publications

For information on installing SuperStack II, Linkbuilder FMS and FMS II hubs, please refer to the user guide which accompanied the hub.

Remote Management

The SuperStack II Hub 10 Management Module and the SuperStack II Hub 10 Advanced RMON Module use SNMP (Simple Network Management Protocol). This can be accessed by remote network management facilities. 3Com has a range of network management products called Transcend.

For details of SuperStack II Hub 10 management using the UNIX- or Windows-based Transcend range, please refer to the appropriate manual:

Transcend Enterprise Manager for UNIX
(Part No. DUA2785-0AAA0X).

Transcend Workgroup Manager for Windows
(Part No. DUA1500-0AAA0X)

Transcend Enterprise Manager for Windows
(Part No. DUA1501-0AAA0X)

If you are using any other remote management software, refer to the accompanying documentation and read the sections that describe how to manage SNMP devices.

Telnet

If you wish to manage your SuperStack II Hub 10 stack via Telnet you will need to refer to the manual(s) supplied with your Telnet host application as well as this guide.

SNMP

We recommend the following publication for an easy-to-read description of SNMP.

The Simple Book by Marshall T Rose
SBN 0-13-812611-9 (published by Prentice Hall).

Special Messages

A special format indicates notes, cautions, and warnings. These messages are defined as follows.

Notes call attention to important features or instructions.

CAUTION: *Cautions contain directions that you must follow to avoid immediate system damage or loss of data.*

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all instructions carefully.*

Conventions

The following table lists conventions that are used throughout this guide.

"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your terminal screen and details that you enter, for example: `Username`
Keys	When specific keys are referred to in the text, they are called out by their labels, such as "the Return key" or "the Escape key," or they may be shown as [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	Italics are used to denote *new terms* or *emphasis*.

Terminology

The following terms and abbreviations are used in this guide:

Flash EPROM	Electrically Erasable Programmable Read-Only Memory
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange protocol
LED	Light Emitting Diode
LSA	LAN Security Architecture
MAC	Media Access Control
MAU	Medium Access Unit
MIB	Management Information Base
NVRAM	Non-Volatile Random Access Memory
PROM	Programmable Read-Only Memory
RMON	IETF Remote Monitoring MIB.
SLIP	Serial Line Internet Protocol
SmartAgent	Intelligent agent software
SNMP	Simple Network Management Protocol
TCP	Transfer Control Protocol
Telnet	A virtual terminal service protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPS	Uninterruptable Power System

1 INTRODUCTION

Overview

The Management Module and Advanced RMON Module are SNMP-conformant, slide-in modules that can manage an entire stack of units. SmartAgent software in the Modules automatically gather and collate information about the stack. As well as supporting in-band management via a network link, each Module has a serial port which allows out-of-band management.

When installed, the Modules allow you to:

- Monitor and change the configuration of all units in the stack.
- Set up resilient links. You can protect a critical communication link against failure by ensuring that, should the main link fail, a standby link immediately and automatically takes over.
- Implement security features. For example, each user is assigned an access level that determines which management parameters the user can view or modify. Also, end station access can be restricted to a particular port.
- Monitor network performance. The management facility maintains statistics that assist you to monitor the operation of the network and perform predefined actions automatically when thresholds are exceeded.
- Poll other devices on the network.

You can use one of several ways to access the management facility:

- Over the network, using an SNMP network manager, such as Transcend WorkGroup Manager for Windows (3C15000 series). Each network manager provides its own user interface to the management facilities. Using SNMP management, for example, you can configure traps to be sent to the management station if critical thresholds are exceeded. You can use SNMP running over the IP or IPX protocols.

- By connecting a VT100 terminal (or workstation with terminal emulation software) to the serial port on the Module. The terminal can be connected directly or remotely, via a modem. The VT100 management interface, which is a menu-driven user interface built into the Modules, is used. The VT100 management interface provides a subset of the features of SNMP management.
- Over a TCP/IP network, using a workstation running VT100 terminal emulation and Telnet. The VT100 management interface is used.
- By connecting a workstation running SLIP to the serial port, which allows you to use out-of-band Telnet or SNMP management. The workstation can be connected directly or remotely, via a modem. This method provides a way of managing the stack in situations where the LAN is not providing a reliable service, or where the network manager does not have direct LAN connectivity.

Any changes made to the configuration of a device using one method of access will be reflected in the configuration seen by all other methods of access.

Using SNMP management, you can access RMON statistics for a stack. Adequate statistics for most situations will be stored by the SuperStack II Hub 10 Management Module (3C16630A). If you want to perform extremely comprehensive RMON analysis on heavily loaded networks, you should consider using the SuperStack II Hub 10 Advanced RMON Module (3C16632).

There is no functional difference between the two types of module. All software will work with both modules as described in this manual. See Appendix A for the specification of each module.

Stacking Units

You can manage a stack containing a mixture of SuperStack II Hub 10 , LinkBuilder FMS, FMS II, 10BT and 10BTi units.

A stack can consist of up to eight units linked together with hub expansion cables (3C625). A stack behaves as a single Ethernet repeater. Only one Management Module or Advanced RMON Module is needed to manage the stack.

If your stack consists of mixed units, the LinkBuilder FMS, 10BTi and 10BT units may ONLY occupy positions 2 through 4.

The Management Module or Advanced RMON Module should be installed in the top or bottom unit. The unit with the module installed is always designated unit 1 in the stack, the next connected unit is unit 2, and so on. The Module records configuration information (such as resilient link settings) for all the units in the stack.

Some SNMP network management applications assume that unit 1 is at the top of the stack. If you install the module in the bottom unit, the stack may be depicted by the application in reverse order to the actual arrangement of units.

The narrower FMS units, if used, should be positioned at the top of the stack.

If you have a stack containing both a LinkBuilder 10BTi unit and a Hub 10 unit fitted with a Module, the Module will manage the stack. The management facilities of the 10BTi unit will be disabled.

SuperStack II Hub 10 Management Module

The SuperStack II Hub 10 Management Module (3C16630A) can be installed in the following units:

3C16665A	**SuperStack II Hub 10 6 Port Fiber**
3C16670A	**SuperStack II Hub 10 12 Port TP**
3C16671A	**SuperStack II Hub 10 24 Port TP**
3C16672A	**SuperStack II Hub 10 24 Port Telco**

This module can be installed in the earlier LinkBuilder FMS II units also.

SuperStack II Hub 10 units support an optional, redundant backup power supply that can help to reduce total power failures.

The module supports all nine groups of RMON.

SuperStack II Hub 10 Advanced RMON Module

The SuperStack II Hub 10 Advanced RMON Module (3C16632) can be installed wherever its companion module (3C16630A) may be used, including the earlier LinkBuilder FMS II modules. See the list above.

The module supports comprehensive, highly accurate, advanced RMON statistics for heavily loaded networks.

2 INSTALLATION AND SETUP FOR MANAGEMENT

Safety Information

WARNING: *Please read the following safety information before installing the Management Module or Advanced RMON Module.*

Installation and removal of either Module should be carried out by qualified personnel only.

Read and follow the Safety Information for the installation and removal of the SuperStack II unit. This can be found in the user manual for the unit.

You must disconnect all the units in the stack from the mains power supply before installing the Module.

The Modules contain static-sensitive components that can be irreparably damaged by static generated by the human body. **Do not touch the components on the circuit board.** Ensure that you only handle the Module by holding it by the edges. We recommend that wherever possible you use a wriststrap or other earthing method whilst installing or removing the Module, to prevent damage by static discharge.

Installing the Management or Advanced RMON Module

WARNING: *You can only install the Hub 10 Management Module or Advanced RMON Module in a Hub 10 or LinkBuilder FMS II unit. If you attempt to install either Module into a LinkBuilder FMS unit, you will damage both products. The section "SuperStack II Hub 10 Management*

Module" on page 1-15 lists the units into which you can install the module.

To complete the installation, you will need a small cross-bladed screwdriver. The installation comprises the following steps:

- Unpack the Hub 10 Module from the carton.
- Disconnect all the units in the stack from the mains power supply. Disconnect the unit into which you will fit the module from the other units.
- Position the unit so that you have enough space in which to work. Remove the blanking plate from the rear panel.
- Insert the module and connect it to the unit.
- Reinstall and power up all the units in the stack, as described in the section "Power Up Sequence" on page 2-6.

Unpacking

Remove the Hub 10 Module from its packaging, taking care not to touch any of its components or connectors. In addition to this manual, the package should contain:

- The Hub 10 Module (as ordered)
- 1x M2.5x25 cross-head screw and crinkle washer

If any of these items are missing, please contact your supplier.

Disconnecting the Unit

1. Disconnect all the units in the stack from the mains power supply. Warn any network users connected to the repeater before you power down the units.

2. Disconnect the unit into which you will fit the module from the other units in the stack. If necessary, move the unit so that you have sufficient space to work.

Removing the Blanking Plate from the Hub 10 Unit

1 Remove the Management Module blanking plate from the rear panel of the unit by unscrewing the three retaining screws (see Figure 2-1). Keep two of the screws for use with the Module. Do not remove any of the screws around the connector ports.

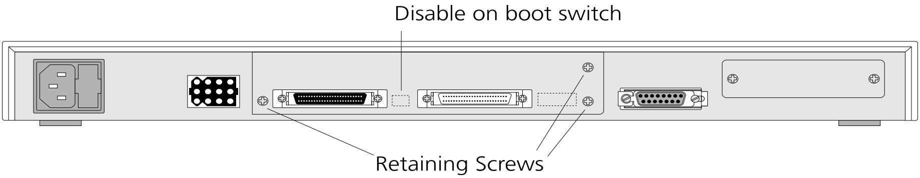


Figure 2-1 Hub 10 Rear View

2 Keep the blanking plate and the remaining original screw in a safe place. If you remove the Module, you must replace the original blanking plate to aid the circulation of cooling air and prevent the entry of dust and debris into the unit.

Inserting the Hub 10 Module

CAUTION: Before you install the Module, *set the position of the Disable-on-Boot switch on the Hub 10 unit. If you want to set up resilient links, change the position from the factory default 'E' (enable all ports) to 'D' (disable all ports'). See the user guide for the Hub 10 unit for details. To manage Resilient Links, see "Port Resilience" on page 3-39.*

1 With the components facing downwards, locate the Module in the guide rails near the top of the unit. Slide the module half way into the unit.

2 Refer to Figure 2-2. Using the insert/remove tab attached to the connector (A), push the connector into the socket (B) on the card below the Module. The connector has a lip on the upper face. Ensure that the lip is facing upwards, and that the pins in the socket align correctly with the connector. Push the connector in fully.

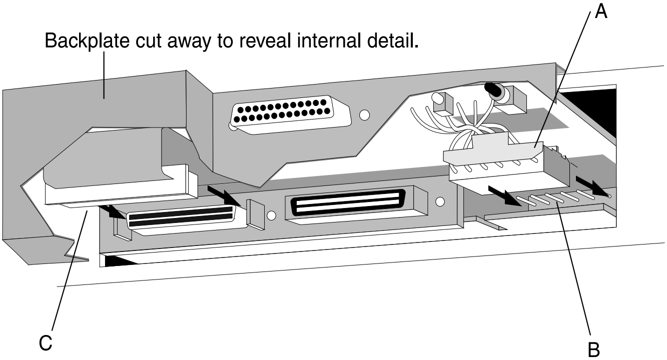


Figure 2-2 Inserting The Hub 10 Module

WARNING: *During installation, both the insert/remove tab and the lip on the connector must be facing the module's printed circuit board (see Figure 2-3). This means that the connecting wires will be twisted as shown in that illustration below. Failure to ensure that the connector is correctly oriented can result in damage to the module when the unit is powered up.*

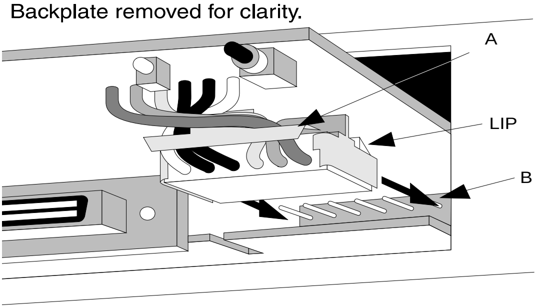


Figure 2-3 Detail Of The Hub 10 Connector

3 Connect the management connector (C) to the unit expansion connector directly below it on the unit. Make sure the connectors are fully pushed in.

4 When the connectors are in place, slide the Module home fully into its slot, taking care not to snag the connecting wires.

5 Secure the module using the supplied longer screw and washer on the left-hand side of the cover, and the two original retaining screws on the right-hand side of the cover.

6 Return your Hub 10 unit to its usual position. If your Hub 10 unit is part of a stack, reconnect the units using the hub expansion cables, starting with the management unit. Connect the OUT port of the management unit to the IN port of the next unit in the stack. Connect the OUT port of the next unit to the IN port of its neighbor. Continue in this manner until all the units in the stack are connected. You can now power up the stack, as described in the section "Power Up Sequence" on page 2-6.

Removing the Hub 10 Module

If you need to remove the module, perform the following steps:

1 Disconnect all the units in the stack from the mains power supply. Disconnect the unit with the Module from the other units in the stack.

2 Unscrew the three module retaining screws and slide the Module partly out to expose the connecetors.

3 Disconnect the management connector.

4 Disconnect the module's power connector by pulling gently but firmly on its insert/removal tab.

5 Slide the module out from the unit.

6 If you are not fitting another module, replace the original blanking plate to aid the circulation of cooling air and prevent the entry of dust and debris into the unit. Use the two shorter retaining screws you have just removed, plus the screw kept with the original blanking plate.

Power Up Sequence

When any unit in the stack is powered up, the Module will reset all the units in the stack. Therefore, to avoid an unnecessary number of resets, power up any other units in the stack before powering up the unit containing the Module.

Connect the mains power cable to the unit with the Module installed, and switch on at the mains socket. The module will perform tests on all units in the stack, and the unit will run through its self-test sequence. This may take up to 20 seconds. The MGMT LED on the front panel of the unit will flash during the self-test.

At the end of the self test:

- The MGMT LED on the front panel of the management unit will light up steady green.
- The appropriate UNIT number LED on each unit in the stack will light.

If the MGMT LED is off, colored red or flashing, refer to "LEDs and Reset Button" on page 2-7.

As a default, the Module powers up the unit with:

- A null IP address.
- The serial port set to autoconfiguration. (Autoconfiguration applies to baud rate only. Parity, character size and stop bits are fixed.)
- All ports enabled.

The unit will function normally but you may need to configure some of these parameters before you can manage the unit, as explained in the sections "Connecting Management Equipment to the Serial Port" and "Managing over the Network" later in this chapter.

LEDs and Reset Button

Two LEDs indicate the state of the Module: a red/green LED on the front panel of the management unit and an amber LED at the rear of the Module. The Reset button is situated at the rear of the Module.

Front Panel MGMT LED

The LED marked *MGMT* on the front panel of the management unit shows the status of the installed Module.

Green (steady) — The Module is operational and no problems are indicated.

Green (flashing) — Software is being downloaded (see "Software Upgrade" on page 3-50) or a self-test is being performed (see "Fault Log" onpage 3-47).

Red — A fault has been identified. If the agent software image is corrupted, the Module will automatically try to reload the software image from the last configured download.
Reset the unit (see "Rear Panel Configure LED and Reset Button").

Off — There is no Module installed in the unit, or the unit cannot identify the installed module. Check that you have installed the module correctly and that the connector cable is secure.

If the measures suggested above fail to rectify the problem, please contact your supplier for further advice.

Rear Panel Configure LED and Reset Button

The rear panel of the Module has a single amber LED (referred to as the Configure LED) and a Reset button. Pressing the Reset button causes the Module to be reset. This has the same effect as executing the Reset command (see "Reset" on page 3-48). The Configure LED will go on for a few seconds after the Reset button is pressed.

Connecting Management Equipment to the Serial Port

This section describes how to connect and set up equipment to communicate with the Module via the serial port (out-of-band management).

By default, the Module will automatically configure its baud rate. You will need to set the character size (8), stop bit (1) and parity (none) settings of the connected equipment to work with the Module.

Connection to the serial port may be direct or through modems, giving the options of local or remote management. The maximum rate the autoconfiguration function will detect is 9600 baud.

Cables of the appropriate type for connection to the serial port should be available from your supplier. If you wish to make up your own cables, refer to the pin-outs given in Appendix A.

Chapter 3 describes the VT100 management interface in detail.

Connecting a VT100 Terminal

To connect a VT100 terminal directly to the serial port, you need a standard null modem cable. See Appendix A for the pin-out information. Connect one end of the cable to the serial port on the Module, and the other to the serial (RS232) port on the VT100 terminal. The Module automatically configures its baud rate as described above, but you must set the character size (8), stop bit (1) and parity (none) settings of the connected equipment to work with the Module.

Refer to "Getting Started" on page 3-6 for details of how to get started with the VT100 management interface.

Connecting a VT100 Terminal Emulator

The workstation will need to run suitable terminal emulation software. Many VT100 terminal emulation packages are available. Refer to the user manuals of your particular terminal emulation package for details, or consult your supplier if you need further advice.

If you are using a PC, you need a null modem cable with an appropriate connector.

The Module automatically configures its baud rate to that of the terminal emulator, as described above. You must set the character size (8), stop bit (1) and parity (none) settings of the emulator to work with the Module. Refer to "Getting Started" on page 3-6 for details of how to get started with the VT100 management interface.

Connecting a Workstation Running SLIP

You can communicate with the Module via the serial port from a workstation running SLIP (Serial Line Internet Protocol). In this way, you can manage the stack using Telnet or SNMP out-of-band management.

The cables you require to connect the workstation will depend on its manufacturer and model. The general guidance given above for terminals will be useful here. You must also configure your workstation to use SLIP. Consult the operator manuals of your workstation for details.

You must configure the serial port of the Module to accept SLIP. This involves setting up the SLIP parameters (address and subnet mask). You can set up the SLIP parameters using either a network connection or a serial port connection. Refer to "IP Addresses" on page A-5 if you are unsure of the values to use. The section "Setup" on page 3-10 explains how to set the parameters using the VT100 management interface.

Refer to "Getting Started" on page 3-6 for details of how to get started with the VT100 management interface.

Managing over the Network

This section describes how to set up equipment to allow you to communicate with the Module over the network (in-band management).

Quick Start for SNMP Management Users

This section describes briefly how to get started if you wish to use an SNMP manager, once you have installed and powered up the Module. It assumes you are already familiar with SNMP management. Refer to the sections which follow for more details. Appendix A contains more information about IP and IPX addresses.

- If you are using the IPX protocol, the Module will be allocated an IPX address automatically. You can start the SNMP manager and begin managing the stack.
- If you are using IP and have a BootP server on your network, the IP parameters will be automatically loaded and brought into use.
- If you are using IP and no BootP server, you will need to configure the stack's IP parameters before the SNMP manager can communicate with the stack. To do this, perform the following steps:

1. Connect a VT100 terminal (configured to 9600 baud, character size 8, stop bit 1, parity none) to the Module's serial port.
2. Log on to system (see "Logon" on page 3-7).
3. Select Management Setup from the Main Menu. (See "Main Menu" on page 3-9.)
4. Use the Management Setup screen (see "Setup" on page 3-10) to enter the IP parameter details.
5. Reset (see "Reset" on page 3-48) the Module. You can now begin managing the stack with the SNMP manager.

Using Telnet

Any Telnet facility that emulates a VT100 terminal should be able to communicate with the Module over the network. Up to three active Telnet sessions can access the Module concurrently. If a connection to a Telnet session is not closed, but is lost inadvertently, the connection will be closed by the Module after between 2 and 3 minutes of inactivity.

To set up Telnet communications, you first need to connect to the Module using serial port access and enter certain parameters.

If you wish to use the VT100 interface to set up parameters including trap addresses, perform the following steps.

1 Connect a VT100 terminal or emulator to the serial port, and logon using the VT100 interface as described in "Getting Started" on page 3-6.

2 Display the Setup screen. Enter the Device IP Address and Device SubNet Mask of the stack, and the Default Router address if necessary, if you know them. If you have a BootP server on your network and wish to assign the details automatically, you may use the BootP facility. Refer to the documentation with your BootP server and "Setup" on page 3-10 for details of how to do this.

3 Logoff from the VT100 interface.

You can now start a Telnet management session. Make sure that your Telnet application is emulating a VT100 terminal. To open the Telnet session, you must specify the IP address of the stack that you entered in step 2 above. Check the user manual supplied with the Telnet facility if you are unsure how to do this.

Once the connection is established, you will see the main banner of the VT100 management interface and you may log on. The VT100 management interface is described in detail in Chapter 3.

Using an SNMP Network Manager

The Transcend WorkGroup and Enterprise Network Management Applications will enable you to get the best out of your SuperStack II Hub 10 units. Any SNMP based network manager can manage SuperStack II Huub 10 and LinkBuilder FMS Series units, provided the MIB (Management Information Base) is installed correctly at the management station. The MIB defines what information is available from the stack through the Module, how that information is structured, and how the SNMP network manager can read and update it.

The use of 3Com network managers is not described in detail in this manual. For more information, contact your supplier.

To manage the stack with an SNMP network manager from another vendor, you need to use the appropriate MIB file. The concise SNMP MIB file for the SuperStack II Hub 10 Series is available free on the Ask3Com bulletin board (see Appendix B).

Refer to the manual accompanying your chosen network manager for details of how to proceed. If you wish to set up SNMP traps, in some cases you may have to configure the Module locally.

3Com network managers such as Transcend WorkGroup Manager for Windows can automatically configure the Module to send traps to them.

To set up SNMP communications, you first need to connect to the Module using serial port access and enter the IP configuration of the stack. Use the VT100 interface to set up parameters including trap addresses. Perform the following steps:

1. Connect a VT100 terminal or emulator to the serial port and logon using the VT100 interface. Refer to "Getting Started" on page 3-6 for details of how to do this.

2. Display the Setup screen (see "Setup" on page 3-10). If using IP, enter the Device IP Address and Device SubNet Mask of the stack, and the Default Router address if necessary, or use the BootP facility (see "Using Telnet" on page 2-10). If using IPX, the stack will have an address automatically allocated.

3. Display the Trap Setup screen (see "Trap Setup" on page 3-13). Enter the IP or IPX address of each network manager that you want to receive traps.

4. Logoff from the VT100 interface.

5. Reset the Module (see "Reset" on page 3-48) to bring the IP parameters into operation.

   You can now start a management session from the SNMP workstation.

3 USING THE VT100 MANAGEMENT INTERFACE

Introduction

This chapter starts with an overview of the VT100 user interface. It describes the screens and how to navigate between them. A map of all the screens is given, to help you to access any chosen screen.

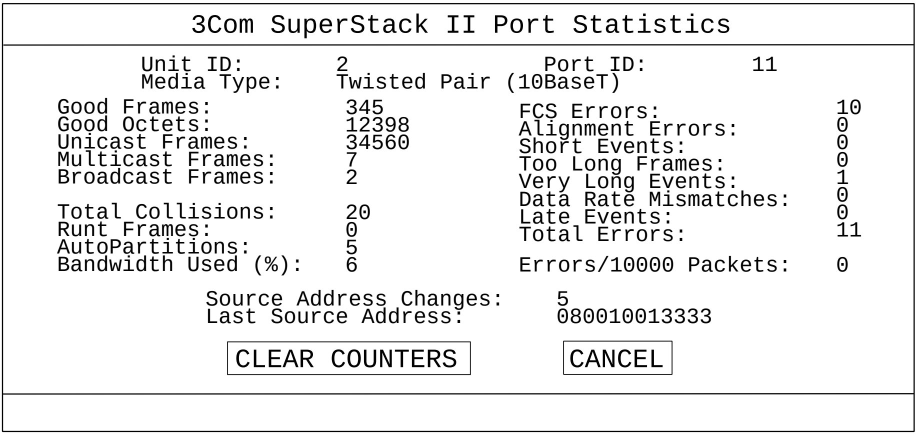
The remainder of this chapter is divided into sections that cover management tasks. These sections broadly follow the division suggested by the main menu. Each screen is described, and the access level needed to access the screen is indicated. Access levels are a security measure, and are described in "Logon" on page 3-7.

User Interface

We suggest you read through this section before you use the facility for the first time. After, you should only need it for reference.

Screens

An example of a VT100 management screen is shown below.



```
                   3Com SuperStack II Port Statistics

           Unit ID:        2               Port ID:        11
           Media Type:     Twisted Pair (10BaseT)

     Good Frames:            345            FCS Errors:                10
     Good Octets:            12398          Alignment Errors:          0
     Unicast Frames:         34560          Short Events:              0
     Multicast Frames:       7              Too Long Frames:           0
     Broadcast Frames:       2              Very Long Events:          1
                                            Data Rate Mismatches:      0
     Total Collisions:       20             Late Events:               0
     Runt Frames:            0              Total Errors:              11
     AutoPartitions:         5
     Bandwidth Used (%):     6              Errors/10000 Packets:      0

                Source Address Changes:     5
                Last Source Address:        080010013333

                 CLEAR COUNTERS             CANCEL
```

Figure 3-1 An Example Screen

Screens are divided into three main areas:

- The header area, at the top of the screen, displays a title which tells you the subject of the screen.
- The main part of the screen shows management information. The components of this part of the screen are described in "Screen Components" on page 3-2.
- The message area, at the bottom of the screen, is used to display information and error messages.

The displayed screens may not be identical to those illustrated in this chapter. The contents of screens depend on your access level and the configuration at your installation. Access levels are described in the section "Screen Components" on page 3-2 .

Screen Components

The main part of a typical screen contains several different types of item. Table 3-1 gives an example of each component, and explains its use.

In the descriptions of the options given in this chapter, the default values are underlined.

Table 3-1 Screen Components

Component	Type	Description
`◆Enabled◆`	Choice Field	Text enclosed in markers is a list, from which you can select one option only. To cycle through the options, press [Space].
`[005634]`	Entry Field	Text enclosed in square brackets on the screen is an Entry Field. An Entry Field allows you to enter different types of data from the keyboard. This may be text, decimal or hexadecimal data. In some cases an Entry Field will have a default entry. To replace the default, simply type in a new value for this field. The default entry will be erased. Password entry fields are hidden, which means that the characters you type are not shown on the screen. To delete a single character, use [Delete] on a VT100 terminal or [Backspace] on a PC.
`Address:`	Read-only information	Text not enclosed in markers or square brackets is information that you cannot change.
`OK`	Button	Text for a button is shown in upper-case letters. A button carries out an action. A menu screen such as the Main Menu consists of a number of buttons arranged in a column. Other screens have a row of buttons at the bottom. To actuate a button, move the cursor to the button and press [Return]. The OK and CANCEL buttons appear on many screens. OK updates the stack according to the data in the fields of the screen, then returns you to the previous screen. CANCEL returns you to the previous screen without applying any changes

`monitor`
`manager`
`security`
	List Box	A list box allows you to select one or more items from a list. Selected items are indicated by an asterisk (*) next to the item.
		To select a single item, move the cursor (using the arrow keys) until the item is highlighted, then press [Return].
		To select more than one item: for each item, move the cursor until the item is highlighted, then press [Space] to select the item. (Pressing [Space] again deselects the item). When all the desired items are selected, press [Return].

Special Keystrokes

As well as the keystrokes described above, there are several other keystrokes for controlling the VT100 interface. These keystrokes allow you to move the cursor around the screen, enter information and move from one screen to another.

[Tab]	Moves the cursor from one field to the next.
[Ctrl]+[B]	Moves the cursor to the next button.

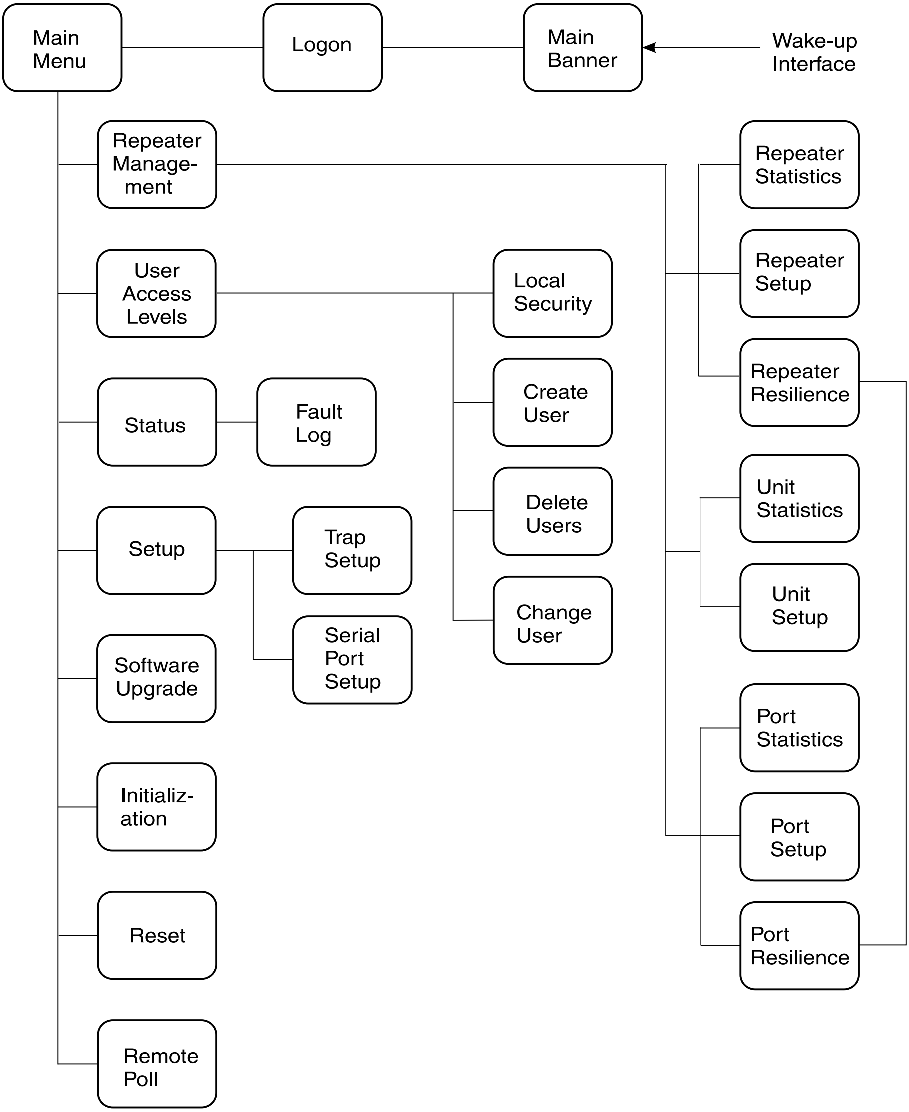
When you have finished entering or changing data, [Ctrl]+[B] is very useful for skipping over the remaining fields.

[Ctrl]+[P]	Returns you to the previous screen without actioning any inputs.
[Ctrl]+[R]	Refreshes the screen.
[Ctrl]+[K]	Displays a list of the possible keystrokes.

If you are using Telnet or a terminal emulation program, you may find that some control keys do not operate, or that they activate other functions. The Windows terminal emulator uses [Ctrl] + [H] as backwards deletion, whereas others use it for backward cursor movement. Consult the manual accompanying your Telnet or terminal emulation software before using the control keys.

Screen Map

This diagram shows how the menus are related to each other.



Getting Started

This section covers logging on to the facility, displaying the main menu and logging off.

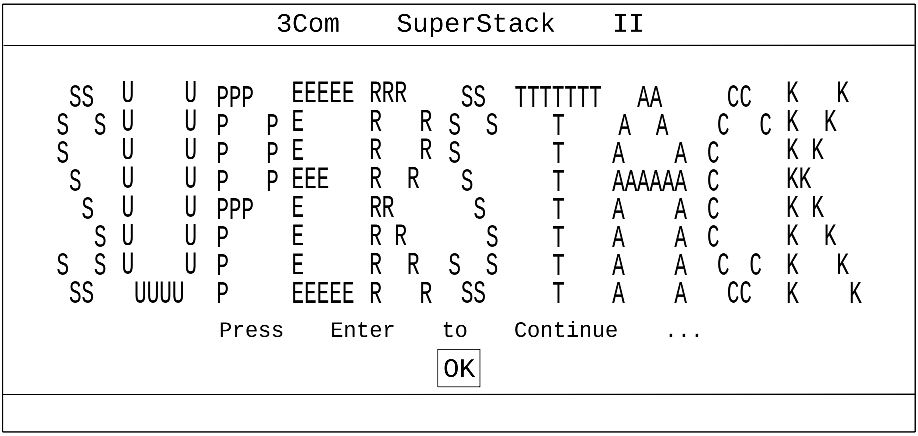
Main Banner

If you are using a VT100 terminal connected (directly or via modems) to the serial port, you need to perform the wake-up procedure. To do this, type [Return] [Return] at the terminal.

By default, the Module will automatically configure the baud rate of the serial port to operate with the connected terminal or modem, provided the parity, stop bits and character size are identical.

If you are using Telnet or SLIP, the wake-up procedure is performed automatically.

When the wake-up procedure is successfully completed, the main banner is displayed.



```
                 3Com    SuperStack    II

 SS  U     U PPP   EEEEE RRR    SS   TTTTTTT  AA      CC   K   K
S  S U     U P   P E     R   R S   S    T    A  A     C   C K  K
S    U     U P   P E     R   R S        T    A    A  C     K K
 S   U     U P   P EEE   R  R    S      T    AAAAAA  C     KK
  S  U     U PPP   E     RR        S     T    A    A  C     K K
   S U     U P     E     R R       S    T    A    A  C     K  K
S  S U     U P     E     R  R   S  S    T    A    A   C C  K   K
 SS   UUUU   P     EEEEE R   R  SS     T    A    A    CC   K    K
              Press    Enter    to    Continue    ...
```

Figure 3-2 Main Banner Screen

The main banner screen has a concealed field which can be revealed using an SNMP manager, by entering text in the sysName MIB object. This field is convenient for defining the Module you are accessing.

If you cannot see the main banner or it displays incorrectly, it may be that:
Your terminal is not configured as a VT100 terminal.
Check that your terminal is setup to operate with acceptable parameters for the serial port (see the section "Serial Port Setup" on page 3-15). The autoconfigure option will only operate if your terminal uses correct parameters for the Module. The maximum speed is 9600 baud.

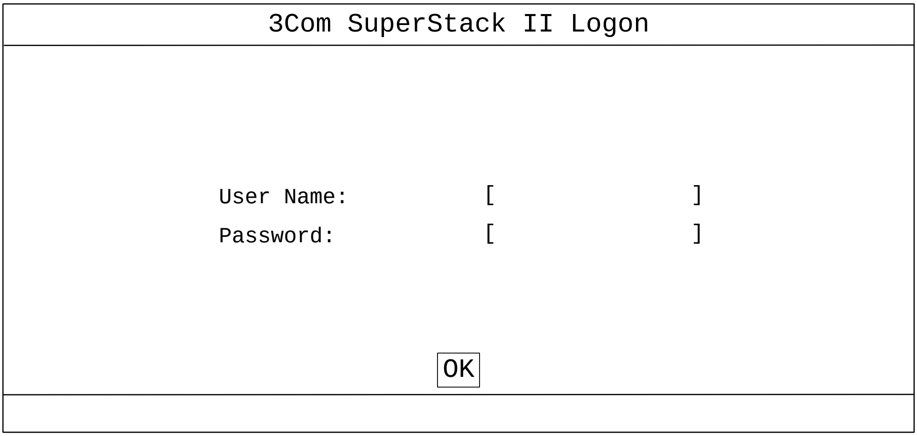
Autoconfigure is disabled.
If you are unable to obtain the banner screen, it is possible that the autoconfigure option has been disabled. Check the configuration of the terminal.

If you cannot resolve the problem, refer to Appendix C for further troubleshooting information.

Once the Main Banner screen is displayed, press [Return] to display the Logon screen.

Logon

You must enter your user name and password to be able to use the management facility. The Logon screen is shown below.



```
                3Com SuperStack II Logon



        User Name:          [                ]
        Password:           [                ]



                          OK
```

Figure 3-3 Logon Screen

If you are logging on for the first time (after installation or initialization), use one of the default user names and passwords shown in Table 3-2. The user name to use depends on which access level you require.

Table 3-2 User Names And Passwords

User Name	Default Password	Access Level
monitor	monitor	monitor You can access but not change the operational parameters of the stack.
manager	manager	manager You can change the operational parameters of the stack but cannot add or delete users, download software or initialize the stack.
security	security	security You can access all the screens and change all manageable parameters.

At the earliest opportunity, the system manager should change the passwords for the default users. The system manager will need to logon as 'manager' and 'monitor' to change their passwords. The section "Edit User" on page 3-21 explains how to change a password.

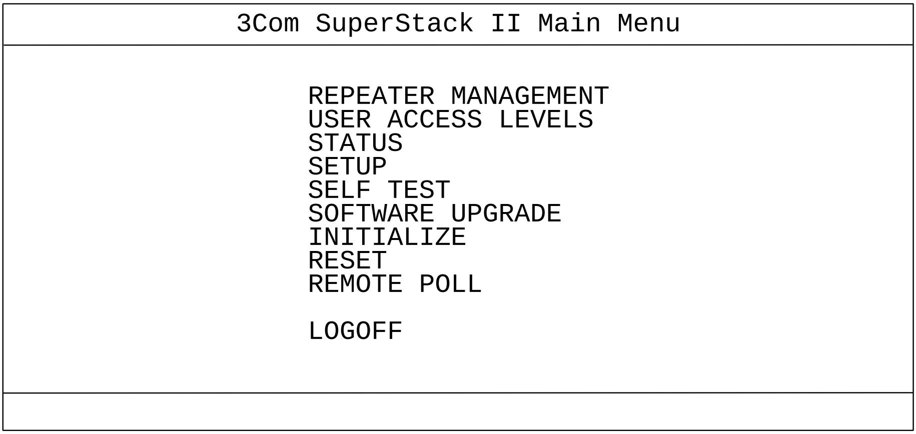
Initializing the stack returns the passwords to their default values (see the section "Initialization" on page 3-49).

If you are not logging on as one of the default users, your system manager will have assigned you a user name and password. The user name determines which of the three access levels (monitor, manager or security) you have.

The user name and passwords are case sensitive. To logon to the facility, enter your user name and password in the appropriate fields and select OK. The Main Menu screen will be displayed.

Main Menu

The Main Menu screen is illustrated below.



```
                3Com SuperStack II Main Menu

                    REPEATER MANAGEMENT
                    USER ACCESS LEVELS
                    STATUS
                    SETUP
                    SELF TEST
                    SOFTWARE UPGRADE
                    INITIALIZE
                    RESET
                    REMOTE POLL

                    LOGOFF
```

Figure 3-4 Main Menu

If you are using the management facility for the first time, we suggest that you:

- Set up logons for any other users and assign each user an appropriate security level. See "Local Security" on page 3-18.
- Assign new passwords for the default users. See "Edit User" on page 3-21.

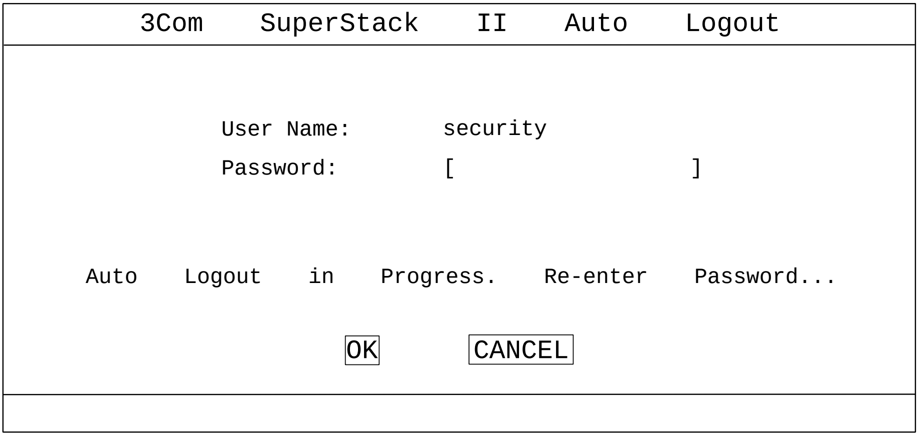
To carry out a particular management task, scroll to the relevant option and press [Return]. The remaining sections of this chapter describe the various Main Menu options.

Logoff

If you have finished using the facility, select the Logoff option from the bottom of the main menu. If you accessed the facility using a Telnet session or modem connection, the connection will be closed automatically.

Auto Logout

There is a built-in security timeout on the VT100 interface. If you do not press any keys for three minutes, the management facility will warn you that the inactivity timer is about to expire. If you do not press a key within 10 seconds, the timer will expire and the screen will be locked. (Any displayed statistics will continue to be updated, however.) When you next press any key, the display changes to the Auto Logout screen. This screen is shown below.



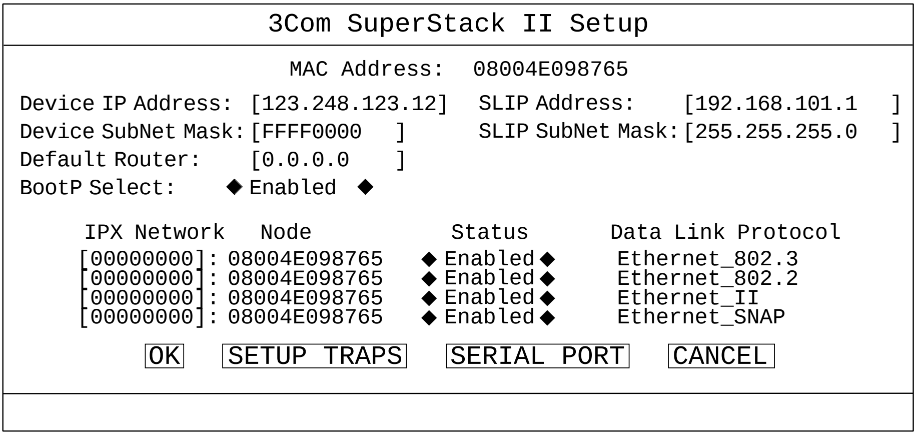
```
          3Com   SuperStack   II   Auto   Logout

                User Name:       security
                Password:        [                  ]

     Auto   Logout   in   Progress.   Re-enter   Password...
```

Figure 3-5 Auto Logout Screen

The Auto Logout screen requests you to enter your password again. If the password is correctly entered, the screen that was active when the timer expired is re-displayed. If you make a mistake in entering your password, you will be returned to the Logon screen.

Setup

You use the Setup screen to configure IP, IPX and SLIP parameters for the stack. This screen also provides access to other screens for you to set up traps and serial port parameters.



```
                      3Com SuperStack II Setup

                   MAC Address:   08004E098765
Device IP Address:  [123.248.123.12]  SLIP Address:     [192.168.101.1   ]
Device SubNet Mask: [FFFF0000     ]   SLIP SubNet Mask: [255.255.255.0   ]
Default Router:     [0.0.0.0      ]
BootP Select:      ◆ Enabled  ◆

     IPX Network    Node           Status      Data Link Protocol
    [00000000]: 08004E098765   ◆ Enabled ◆     Ethernet_802.3
    [00000000]: 08004E098765   ◆ Enabled ◆     Ethernet_802.2
    [00000000]: 08004E098765   ◆ Enabled ◆     Ethernet_II
    [00000000]: 08004E098765   ◆ Enabled ◆     Ethernet_SNAP

         OK    SETUP TRAPS    SERIAL PORT    CANCEL
```

Figure 3-6 Setup Screen

MAC Address (Read-only) The MAC address of the Module. This cannot be changed.

Device IP Address (Text Field) If using IP, you will need to enter a unique IP address for the stack. (See "IP Addresses" on page A-5.) You may use the BootP facility (see below) if your network has a BootP server, or enter it manually. If you do not know the address, consult your network administrator. If you change the device IP address, you must reset the Module to effect the change.

Device SubNet Mask (Text Field) If using IP, enter a suitable subnet mask. BootP will do this automatically. For a class B IP address, 255.255.0.0 is suitable. Check with your network administrator if you are unsure. If you change this field, reset the Module to effect the change.

Default Router (Text Field) If necessary, enter the IP address of the default router on your network. BootP will do this automatically. If you change this field, reset the Module to effect the change.

SLIP Address (Text Field) SLIP (Serial Line Internet Protocol) allows IP to run over the serial port instead of the network. SLIP allows you to use out-of-band Telnet or SNMP management, either locally or remotely via a modem. SLIP will operate with a SLIP address of 192.168.101.1.

If you enter a SLIP address, it should show a different network from the stack that you are managing. Check with your network administrator if you are unsure. If you change this field, reset the Module to effect the change.

If you require more information about SLIP, read the Internet Activities Board document RFC 155

SLIP SubNet Mask (Text Field) Enter a suitable subnet mask. For a class C address, 255.255.255.0 (the default setting) is suitable. Check with your network administrator if you are unsure. If you change this field, reset the Module to effect the change.

If you are using SLIP, ensure that Flow Control is not set to XON/XOFF (see "Serial Port Setup" on page 3-15).

BootP Select (Choice Field) Enabled/Disabled
When enabled, BootP allows you to download the IP address, the SubNet Mask, and the Router IP address from a BootP server on your network. When operative, BootP checks that a valid IP address is not installed before sending out requests for the data. It will keep on sending requests for data until one of three conditions is satisfied:

- BootP is disabled,
- a valid BootP reply is received,
- or, you enter the address manually.

When the IP parameters have been received, the Module will reset automatically. No management commands are possible while the module reboots and self-tests.

The following four fields are used for IPX addressing.

IPX Network (Text Field) This field shows the address of the network for this protocol. This address is learned automatically from the local IPX router or NetWare File Server, and you should not need to change it.

Node (Read-only) This field shows the node address of the repeater stack, which is learned automatically.

Status (Choice Field) Enabled / Disabled
This field shows whether the data link protocol is enabled. Choose *Disabled* if you wish to prevent access for any reason, such as security considerations.

Data Link Protocol (Read-only) This field shows the name of the IPX data link layer protocol.

OK (Button) Press [Return] when the OK button is highlighted to action your selections for this screen. You will be returned to the main menu.

If you have changed the parameters, you will need to reset the Module to effect the changes. Refer to the section "Reset" on page 3-48.

SETUP TRAPS (Button) Press [Return] when the SETUP TRAPS button is highlighted to set up the parameters for traps (see "Trap Setup" below).

SERIAL PORT (Button) Press [Return] when the SERIAL PORT button is highlighted to set up the RS-232C port parameters (see "Serial Port Setup" on page 3-15).

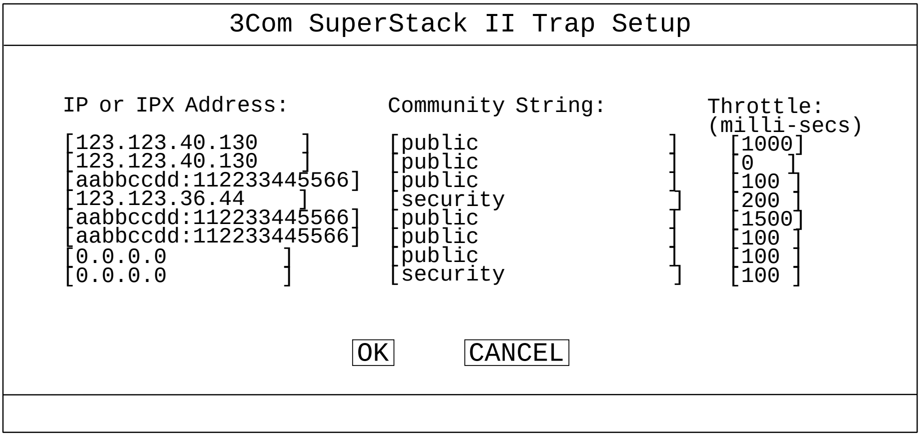
CANCEL (Button) Press [Return] when the CANCEL button is highlighted to abandon this screen without actioning any changes, and return to the main menu.

Trap Setup

Traps are messages sent across the network to an SNMP network manager, such as Transcend WorkGroup Manager for Windows. Traps can alert the system administrator to faults or changes in the stack.

Your Transcend SNMP network manager may automatically set up the trap destination addresses for you. Check the documentation accompanying the product.

You access the Trap Setup screen by selecting the SETUP TRAPS button on the Setup screen.



```
3Com SuperStack II Trap Setup

IP or IPX Address:        Community String:        Throttle:
                                                   (milli-secs)
[123.123.40.130    ]      [public              ]     [1000]
[123.123.40.130    ]      [public              ]     [0   ]
[aabbccdd:112233445566]   [public              ]     [100 ]
[123.123.36.44     ]      [security            ]     [200 ]
[aabbccdd:112233445566]   [public              ]     [1500]
[aabbccdd:112233445566]   [public              ]     [100 ]
[0.0.0.0           ]      [public              ]     [100 ]
[0.0.0.0           ]      [security            ]     [100 ]
```

Figure 3-7 Trap Setup Screen

IP or IPX Address (Text Field) Enter the IP or IPX address of the remote network management station to which SNMP traps should be sent.

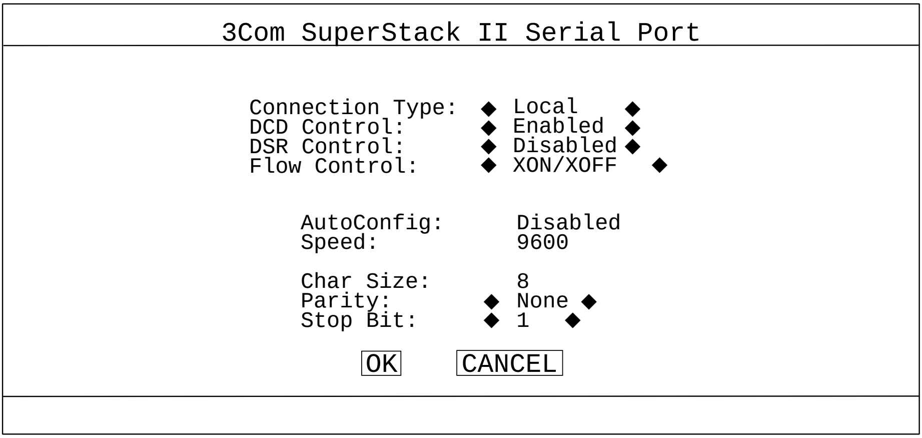
Community String (Text Field) The community string allows a very simple method of authentication between the Module and the remote network manager. You can enter any text string of up to 32 characters (case sensitive!).

The remote network manager must be configured to look for traps sent with this community string, otherwise it will ignore the traps. The default community string is *public*.

Throttle (Text Field) To prevent a remote network manager receiving too many traps at once, you can configure the stack to transmit traps with a delay between each trap. If several traps are generated at once, they will be transmitted with the specified delay between them. The unit of throttle is one thousandth of a second. The default value is 100, which gives a delay of one tenth of a second between each transmission. If you set the throttle to 0, traps will be sent as soon as they are generated.

Serial Port Setup

You can access the Serial Port Setup screen by actuating the SERIAL PORT button on the Setup screen.



```
                3Com SuperStack II Serial Port

        Connection Type:  ◆ Local    ◆
        DCD Control:      ◆ Enabled  ◆
        DSR Control:      ◆ Disabled ◆
        Flow Control:     ◆ XON/XOFF   ◆

            AutoConfig:     Disabled
            Speed:          9600

            Char Size:      8
            Parity:       ◆ None ◆
            Stop Bit:     ◆ 1   ◆
```

Figure 3-8 Serial Port Setup Screen

If you alter the serial port parameters and select OK, you will terminate any existing session using the serial port. Ensure that the connected equipment's serial port parameters are set to match the new configuration. This will allow you to continue to access the management facility using the equipment after you change the serial port parameters.

If you change the serial port parameters with Auto Config already set to *Enabled*, or if you change Auto Config to *Enabled*, you will need to perform the *wake-up* procedure (see "Main Banner" on page 3-6) before communication is re-established.

Connection Type (Choice Field) Local / Remote
Select *Remote* if you want to manage the stack via a modem. DCD Control and DSR Control will be enabled. Otherwise, leave this parameter at the default setting.

DCD Control (Choice Field) Enabled / Disabled
Check in the manual for your modem if you are not sure of the correct setting.

DSR Control (Choice Field) Enabled / Disabled
If DSR Control is enabled, the management port will be logged out if DSR is deasserted. Check in the manual for your modem if you are not sure of the correct setting.

Flow Control (Choice Field)
XON/XOFF / NONE / RTS - CTS Unidirectional / RTS - CTS Bidirectional
Select the flow control option that corresponds with your terminal or modem.

Auto Config (Choice Field) Enabled / Disabled
The Module can automatically configure the terminal speed to work with your VT100 terminal. Note that the setting made by automatic configuration is not displayed on the screen. The displayed setting is that which will be adopted when automatic configuration is next disabled. Set this field to *Enabled* if you require automatic configuration.

To start automatic configuration detecting and setting the correct speed, the *wake-up* procedure (typing [Return] [Return]) must be performed.

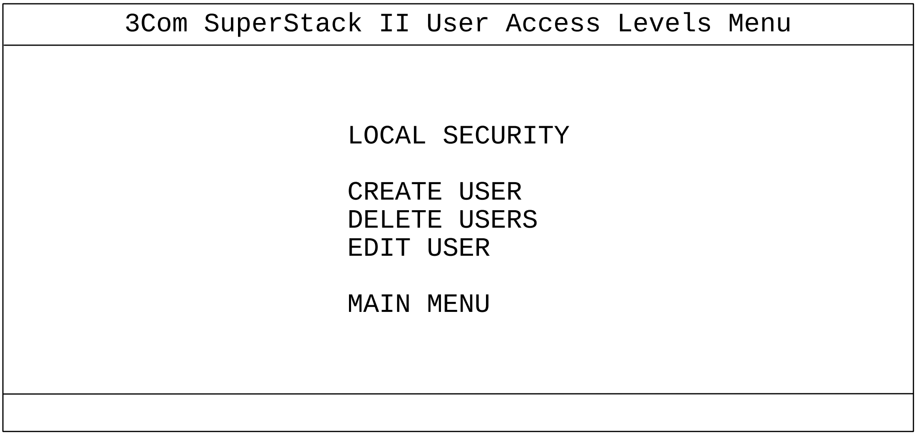
Speed (Choice Field) 1200 / 2400 / 4800 / 9600
Select the baud rate for your terminal or modem. Check in the manual for your terminal or modem if you are not sure of the correct setting.

Char Size (8), Parity (NONE) and **Stop Bit** (1) are fixed.

Attempts to set invalid serial port parameters will be rejected. All parameters will be reset to their default values.

User Access Level

The User Access Level screen provides a menu to access four further screens.



```
3Com SuperStack II User Access Levels Menu

                    LOCAL SECURITY

                    CREATE USER
                    DELETE USERS
                    EDIT USER

                    MAIN MENU
```

Figure 3-9 User Access Level Menu

Local Security This screen allows you to enable or disable access to the management facility, for each combination of access method (serial port, Telnet or SNMP) and access level.

Create User This screen allows you to create another user who can access the management facility, in addition to the default users.

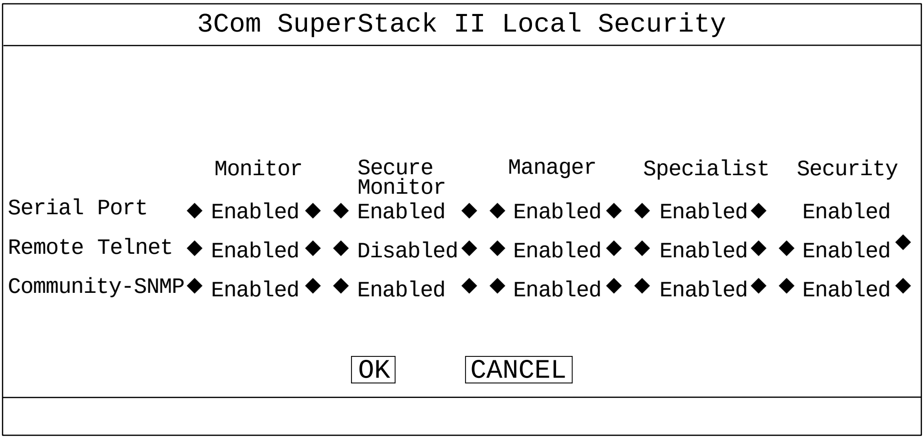
Delete Users This screen allows you to remove users, other than the default users.

Edit User This screen allows you to change your own password and community string.

The first three screens are only available for users with *security* access level. Select the option for the screen you require and press [Return].

Local Security

You can access the Local Security screen by actuating the LOCAL SECURITY button on the User Access Level screen. This option is available only for users with *security* access level.



```
                 3Com SuperStack II Local Security

                    Monitor     Secure      Manager    Specialist  Security
                                Monitor
Serial Port     ◆ Enabled ◆ ◆ Enabled  ◆ ◆ Enabled◆ ◆ Enabled◆    Enabled
Remote Telnet   ◆ Enabled ◆ ◆ Disabled◆ ◆ Enabled◆ ◆ Enabled◆ ◆ Enabled◆
Community-SNMP◆ Enabled ◆ ◆ Enabled  ◆ ◆ Enabled◆ ◆ Enabled◆ ◆ Enabled◆

                              OK        CANCEL
```

Figure 3-10 Local Security Screen

The Local Security screen shows a table displaying every combination of access method (serial port, Telnet or SNMP) and access level. For example, the top left choice field shows whether serial port access by users with *monitor* access level is enabled or disabled.

The access levels are defined as:

- Monitor - This allows the user to view the essential operations of the stack and to establish whether or not the stack is operating correctly. A user at this level cannot change the operating parameters of the stack or gain access to any of the setup menus.
- Secure Monitor - In this implementation, Secure Monitor has the same rights as Monitor.
- Manager - This allows the user to monitor and change the operational parameters of the stack. The user cannot create or delete other users, re-initialize the stack or download a software image.

- Specialist - In this implementation, Specialist has the same rights as Manager.
- Security - This level of security allows a user access to all the management operations. This level of security should be assigned only to the system administrator or somebody with the system administrator's responsibilities.

All the fields are choice fields. The options for each field are *Enabled* (the default) or *Disabled*.

To prevent you from locking yourself out from the stack completely, serial port access is always kept enabled for the *security* access level.

Make any changes you require, then move the cursor to the OK button and press [Return]. Remember that you can use [Ctrl]+[B] to jump to the OK button.

Serial Port (Choice Field) Enabled / Disabled
To prevent access to the management facilities via the serial port, disable access to the facility for each access level. To allow you to configure the stack locally in the event of problems on your network, we suggest that you change the default password (see "Edit User" on page 3-21) for the permanently-enabled security access level.

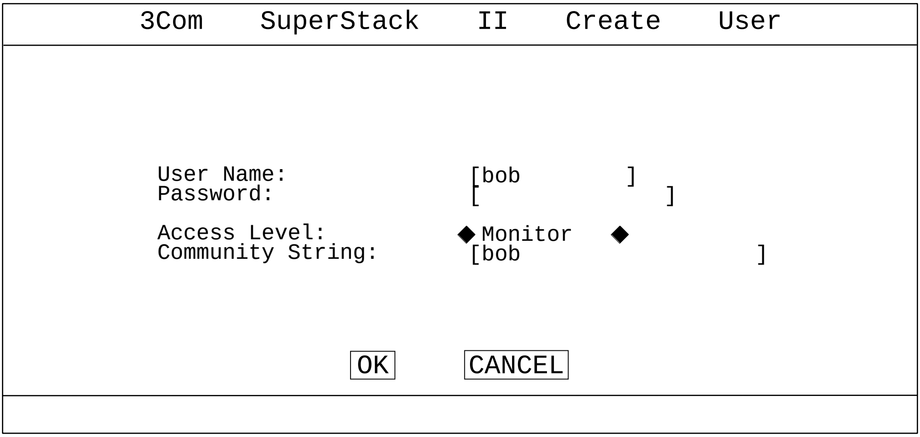
Remote Telnet (Choice Field) Enabled / Disabled
Telnet is an insecure protocol. You may wish to disable all access to the management facilities via Telnet if there is important or secret data on your network.

Community SNMP (Choice Field) Enabled / Disabled
The stack can be managed via SNMP using a remote network manager such as Transcend WorkGroup Manager for Windows. Community SNMP does have some simple security features but it is an insecure protocol. You may wish to disable all access to the management facilities via Community SNMP if there is important or secret data on your network.

Create User

You access the Create User screen by actuating the CREATE USER button on the Security screen. This option is available only for users with *security* access level.

Use this screen to add new users. There can be up to 10 users, including the three default users. Up to three users can concurrently access the management facility using Telnet. There is no limit to the number of SNMP remote management sessions.



```
          3Com    SuperStack    II    Create    User

   User Name:                 [bob        ]
   Password:                  [              ]

   Access Level:             ◆ Monitor   ◆
   Community String:          [bob                  ]
```

Figure 3-11 Create User Screen

User Name (Text Field) Enter the name of the user. The name can be up to 10 characters. The user name is case sensitive.

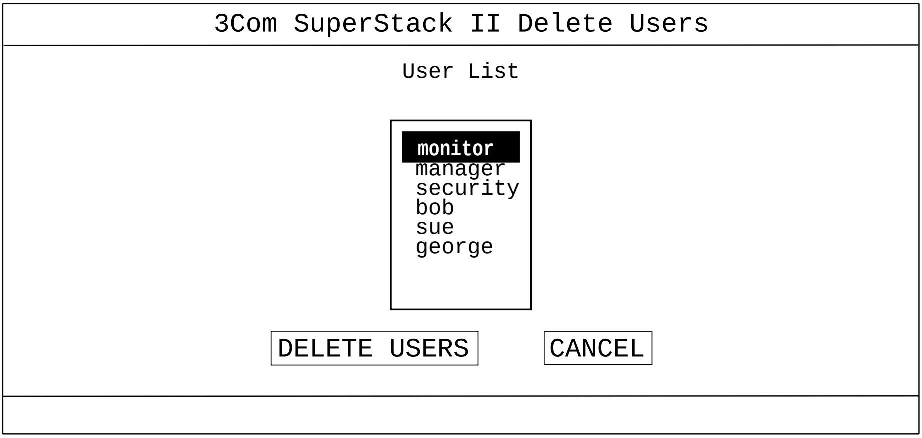
Password (Text Field) Enter a password for this user. The password can be up to 10 characters. The password is case sensitive and will not be displayed on the screen.

Access Level (Choice Field)
Monitor / Secure Monitor / Manager / Specialist / Security
Enter an appropriate access level for the new user by cycling through the options using the space bar.

Community String (Text Field) By default, the community string is the same as the User Name. You can change this string if you wish, to any text string of up to 32 characters. The community string is used only for SNMP access. The remote network manager must be configured to use the same community string.

Delete Users

You access the Delete Users screen by actuating the DELETE USERS button on the Security screen. This option is available only for users with *security* access level.



3Com SuperStack II Delete Users

User List

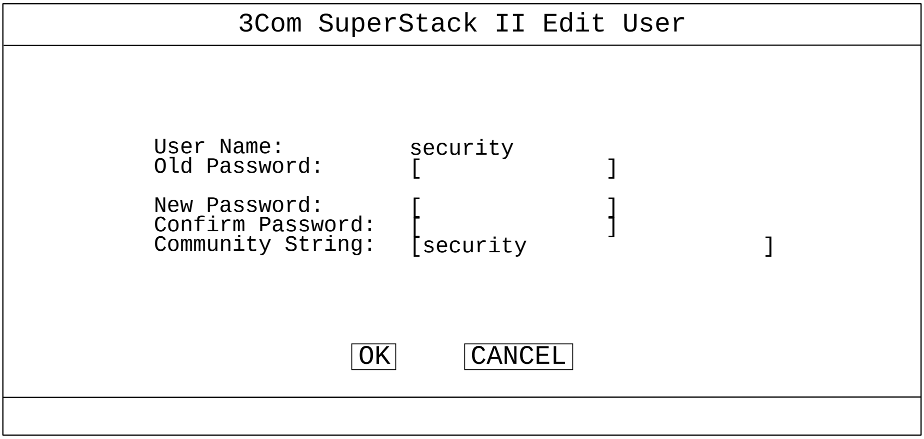
Figure 3-12 Delete Users Screen

Select the users to delete from the List Box using the spacebar, then move the cursor to the DELETE USERS button and press [Return]. You cannot delete the current user (in other words, the user name you used to logon) or any of the default users (monitor, manager or security).

Edit User

You access the Edit User screen by actuating the EDIT USER button on the Security screen. Use this screen to change your own password or community string.

No user can directly change another user's password or community string. If you are a system administrator and wish to change another user's password, you will need to login as the other user.



```
                  3Com SuperStack II Edit User

           User Name:            security
           Old Password:         [               ]

           New Password:         [               ]
           Confirm Password:     [               ]
           Community String:     [security                    ]


                             OK      CANCEL
```

Figure 3-13 Edit User Screen

The options are similar to the Create User screen (see "Create User" on page 3-20). The main differences are the password fields. You must type in your current password in the *Old Password* field before you can change any fields. To set a new password, enter the password in both the *New Password* and *Confirm Password* fields.

If you forget your password, refer to the advice in Appendix C.

Repeater Management

This section is the most important for configuring the stack to operate correctly on your network. There are three levels at which you can manage the stack, and three management activities.

Management Levels

The three management levels are:

- Repeater - If you manage at Repeater level, you are managing or viewing the device as a whole. The device consists of a stack of one to eight units linked together by hub expansion cables to form a single, logical repeater.

- Unit - If you manage at Unit level, you are managing or viewing a single unit in the stack. This can be a Hub 10, FMS, FMS II, 10BT or 10BTi unit.
- Port - Managing at Port level lets you set up parameters and examine statistics for individual ports. This allows you to manage individual users or small workgroups.

Management Activities

The three management activities are:

- Statistics - Viewing statistics on a regular basis allows you to build up a picture of how your network is performing. If you keep simple daily records, you will see trends emerging and soon notice problems arising before they cause major network faults. Statistics can be useful to help you get the best out of your network.
- Setup - Setup allows you to configure various parameters for the repeater, and individual units and ports. In many cases, the default settings are suitable for typical operation, but it may be a advisable to disable unused ports to prevent unauthorized access to the network.
- Resilience - You can configure resilient links, to protect critical communication links against failure.

You select the management level and management activity from the Repeater Management screen. The appropriate screen is then displayed; for example, the Port Resilience screen.

Repeater Management Screen

The fields on the Repeater Management screen change slightly depending on the selected management level. Only relevant fields are displayed. The displayed fields will not change until you move the cursor from the Management Level field.

The flow chart shows the fields you fill in depending on the chosen level of management.

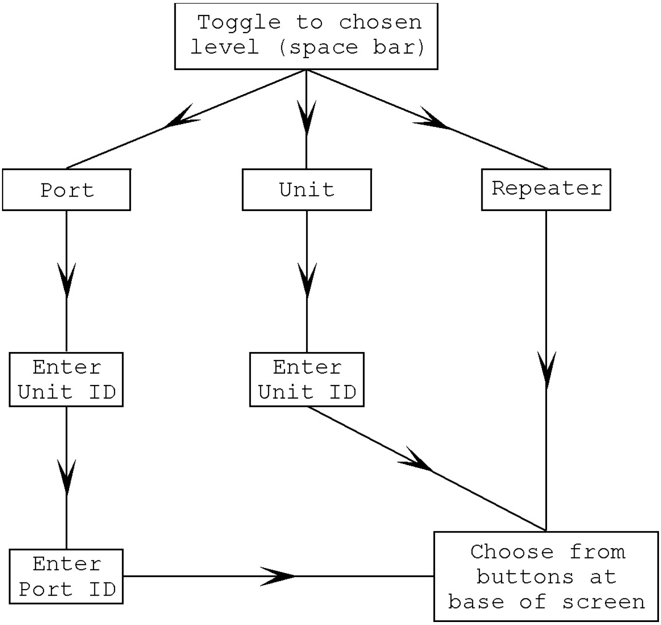
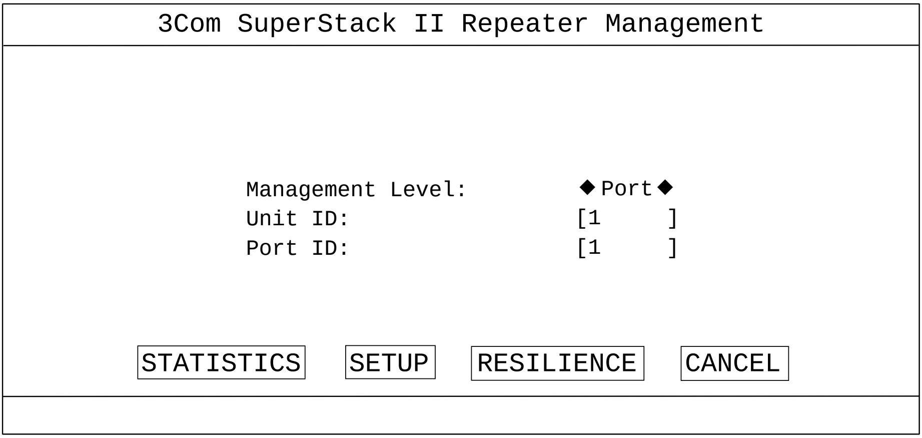

Toggle to chosen level (space bar)
Port
Unit
Repeater
Enter Unit ID
Enter Unit ID
Enter Port ID
Choose from buttons at base of screen

Figure 3-14 Using The Repeater Management Screen

The example screen below shows the screen with port level management selected.



```
                  3Com SuperStack II Repeater Management



              Management Level:          ◆Port◆
              Unit ID:                   [1    ]
              Port ID:                   [1    ]


     STATISTICS    SETUP    RESILIENCE    CANCEL
```

Figure 3-15 Repeater Management Screen

Management Level (Choice Field) Repeater / Unit / Port
Toggle to the level you wish to manage.

Unit ID (Text Field) Enter the identifying number of the unit you wish to manage. The Unit ID is a digit, and is displayed by the Unit LED on the front of each unit.

The unit with the Module installed is unit 1, the next unit in the stack is unit 2, and so on.

If the number entered into the Unit ID field is invalid (that is, the unit is not in the stack), the button choice will be rejected. The same will happen if the Module cannot communicate with a unit whose Unit ID is known to be valid. In this latter case, check the cable connections.

Port ID (Text Field) Enter the identifying number of the port you wish to manage. Table 3-3 provides a summary of port numbering.

Table 3-3 Port Numbering

Unit	Product	Media	Port Numbers	AUI / Transceiver Module (Tcvr)
3C16250	FMS 12 port	Coaxial	1 to 10, left to right	Tcvr: 11, AUI: 13
3C16265	FMS 6 port ST	Fiber	1 to 6, left to right	Tcvr: 7, AUI: 8
3C16271	FMS 12 port RJ45	TP	1 to 12, left to right	AUI or Tcvr: 13
3C16371	FMS 24 port RJ45	TP	top 1 to 12, left to right bottom 13 to 24, left to right	AUI: 25, Tcvr: 26
3C16665	FMS II 6 port ST	Fiber	1 to 6, left to right	Tcvr: 7, AUI: 8
3C16670	FMS II 12 port RJ45	TP	top 1 to 6, left to right bottom 7 to 12, left to right	AUI or Tcvr: 13
3C16671	FMS II 24 port RJ45	TP	top 1 to 12, left to right bottom 13 to 24, left to right.	AUI: 25, Tcvr: 26
3C16672	FMS II 24 port telco	TP	left connector 1 to 12: right connector 13 to 24.	AUI: 25, Tcvr: 26
3C16665A	Hub 10 6 port ST	Fiber	1 to 6, left to right	Tcvr: 7, AUI: 8
3C16670A	Hub 10 12 port RJ45	TP	top 1 to 6, left to right bottom 7 to 12, left to right	AUI or Tcvr: 13

Table 3-3 Port Numbering (Continued)

Unit	Product	Media	Port Numbers	AUI / Transceiver Module (Tcvr)
3C16671A	Hub 10 24 port RJ45	TP	top 1 to 12, left to right bottom 13 to 24, left to right.	AUI: 25, Tcvr: 26
3C16672A	Hub 10 24 port telco	TP	left connector 1 to 12: right connector 13 to 24.	AUI: 25, Tcvr: 26

STATISTICS (Button) Move the cursor to this button and press [Return] to move to the Statistics screen for the management level you have chosen.

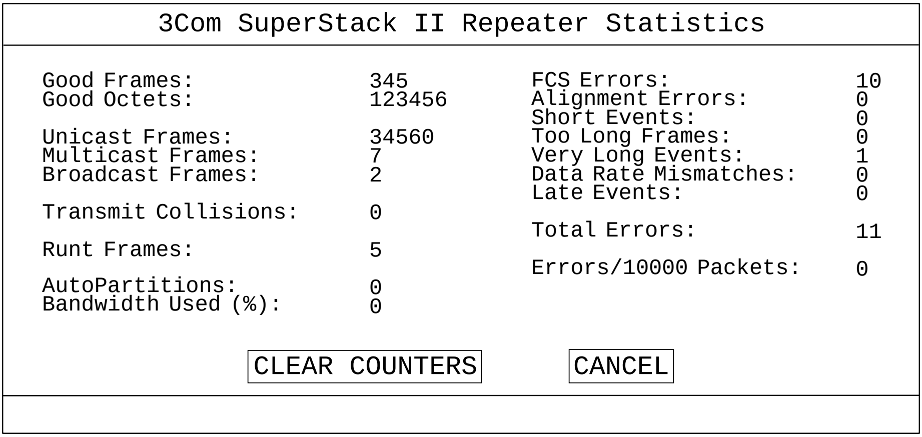
SETUP (Button) Move the cursor to this button and press [Return] to move to the Setup screen for the management level you have chosen.

RESILIENCE (Button) Move the cursor to this button and press [Return] to move to the Resilience screen for the management level you have chosen (either *Repeater* or *Port*). This button is not displayed when *Unit* is selected.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the main menu.

Repeater Statistics

You access the Repeater Statistics screen from the Repeater Management screen, by selecting management level *Repeater* then actuating the STATISTICS button. The statistics given are the aggregated counters for all the ports in all the units in the stack.



```
                  3Com SuperStack II Repeater Statistics

  Good Frames:              345           FCS Errors:              10
  Good Octets:              123456        Alignment Errors:        0
                                          Short Events:            0
  Unicast Frames:           34560         Too Long Frames:         0
  Multicast Frames:         7             Very Long Events:        1
  Broadcast Frames:         2             Data Rate Mismatches:    0
                                          Late Events:             0
  Transmit Collisions:      0
                                          Total Errors:            11
  Runt Frames:              5
                                          Errors/10000 Packets:    0
  AutoPartitions:           0
  Bandwidth Used (%):       0

                  CLEAR COUNTERS          CANCEL
```

Figure 3-16 Repeater Statistics Screen

The screen is updated every 3 seconds. If the top limit of a counter (4294967295) is reached, the counter will *roll-over* (reset to zero automatically). After this event, the individual figures may give a false impression of network conditions if taken in isolation.

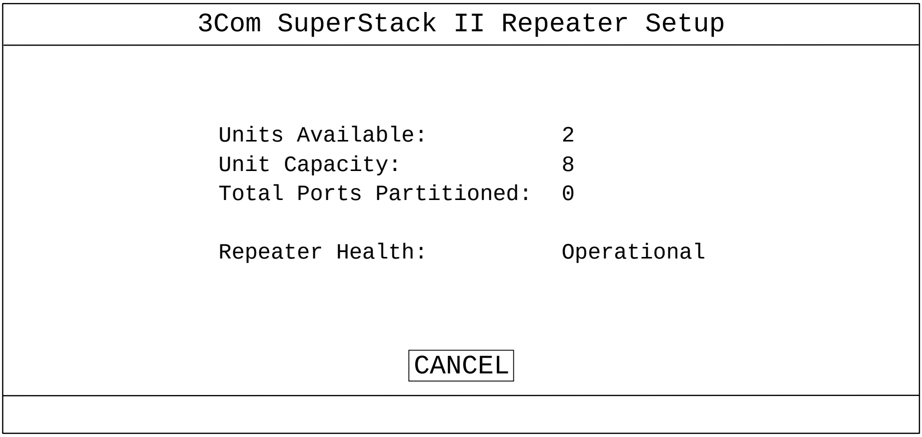
All the fields are read-only. Refer to Appendix D for a detailed description of the statistics fields.

CLEAR COUNTERS (Button) This button is shown only for users with an access level of manager or higher. Select this button and press [Return] to reset all the statistics counters on the repeater to zero. Clearing the repeater counters affects all users, and clears the counters for all the units and ports on this repeater.

CANCEL (Button) Select this button to go back to the Repeater Management screen without clearing the counters.

Repeater Setup

You access the Repeater Setup screen from the Repeater Management screen, by selecting management level *Repeater* then actuating the SETUP button. The Repeater Setup screen shows the current configuration of the repeater (stack).



```
               3Com SuperStack II Repeater Setup

          Units Available:          2
          Unit Capacity:            8
          Total Ports Partitioned:  0

          Repeater Health:          Operational
```

Figure 3-17 Repeater Setup Screen

Units Available (Read-only) This field shows how many units are currently installed in the repeater stack.

Unit Capacity (Read-only) This shows the maximum number of units that can be supported by this stack, in this case eight.

Total Ports Partitioned (Read-only) This field shows the number of partitioned ports.

Repeater Health (Read-only) If all system tests have been passed on start up or during a self-test this field will show *Operational*. If the field is blank or displays any other message, check the Fault Log screen for further information. See "Fault Log" on page 3-47.

Repeater Resilience

Resilient Links can be set up ONLY on Hub 10 and *FMS II units.*

You access the Repeater Resilience screen from the Repeater Management screen, by selecting management level *Repeater* then actuating the RESILIENCE button. The screen shows all the resilient link pairs that are currently configured for the repeater.

Resilient Links are only available on twisted pair and fiber optic media, because the link test pulse or the idle signal is used to decide whether the link is broken and the standby link should be activated. There is no such link signal over coaxial media.

If you have not come across resilience in the networking field before, you will find the following explanation helps.

When a link is broken, all communication between devices on each side of the link is lost. It could be very inconvenient for a manager physically to reinstate the network immediately. Important traffic might be lost. If a spare link could pick up where the broken link left off, the network would appear to function normally to the outside observer. At worst, a few frames would be corrupted or lost.

This is the concept of resilience as applied to ports. One port is on stand-by waiting to take over if the main port fails.

You may set up 16 resilient pairs of ports on one chassis. A pair may be on the same module or on different modules. Each port in the pair can be attached to different media. Each resilient pair consists of a main port and a stand-by port. When the pair is operating normally, the main port carries data to and from the segment attached to the port. However, if the Module detects a loss of link (link test pulse for twisted pair medium) or loss of light (idle signal for fiber optic medium), this main port is disabled and the stand-by port takes over.

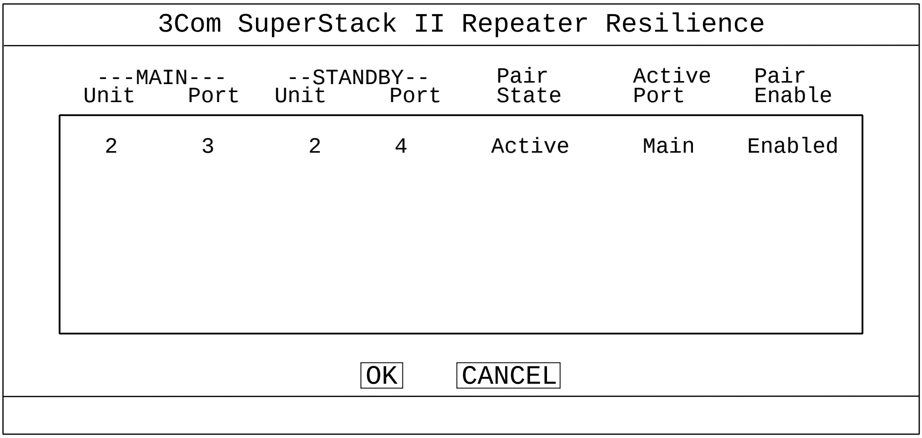
To keep you informed of what is happening on the network, an event or trap will be sent to the Network Manager informing you that a main port has been disabled and a stand-by port has taken over. If you then rectify the fault on the main port, or the fault clears, the operation will switch back automatically to the main port.

It is important to ensure that the unit with the standby port has the hardware switch (see Figure 2-1) in the correct position, that is, in the 'disabled on boot' position. If you are unsure of how to do this, consult the guide that came with the Hub 10 unit. Setting the switch correctly will avoid creating a loop when the power is first applied. The Module will re-configure the ports after power-up.

The Resilience feature is available from VT100, Transcend or another SNMP Manager. Details of how to use the Port Resilience screen are given in "Port Resilience" on page 3-39.

The management facility can only recognize loss of link/light on a local port.
Suitable application of an alarm can activate the resilience feature. If a port is receiving a number of errors, an alarm set on the error counter can trigger change-over to its resilient partner. See Appendix E.

WARNING: *Security may be set up at the same time as Resilience, but only using a network manager.*



```
          3Com SuperStack II Repeater Resilience

     ---MAIN---      --STANDBY--       Pair        Active     Pair
    Unit     Port    Unit      Port    State       Port       Enable

       2       3        2       4      Active       Main      Enabled

                         [OK]     [CANCEL]
```

Figure 3-18 Repeater Resilience Screen

All the fields are read-only. To change the configuration of a resilient link, select the link then select OK. The Port Resilience screen, showing details of the chosen link, will be displayed.

MAIN Unit This field shows the identifier of the unit that the main port belongs to.

MAIN Port This field shows the identifier of the main port.

STANDBY Unit This field shows the identifier of the unit that the standby port belongs to.

STANDBY Port This field shows the identifier of the standby port.

Pair State This field shows the state of the resilient link pair. Possible values are:

- Active - The link pair is enabled, and either the main port or the standby port is capable of carrying traffic.
- Not in use - The link pair is disabled.
- Both Failed - Although the link pair is correctly configured, both links have failed.
- Invalid - The state of the repeater has changed since the link pair was configured, and the link pair now does not conform to the resilient link rules (see “Port Resilience” on page 3-39). An example is where the Disable on Boot switch of the unit with the standby port has been changed to Enable.

Active Port This field shows which port is carrying the traffic: the main port or the standby port.

Pair Enable This field shows whether the resilient link pair is currently enabled or not. Possible values are:

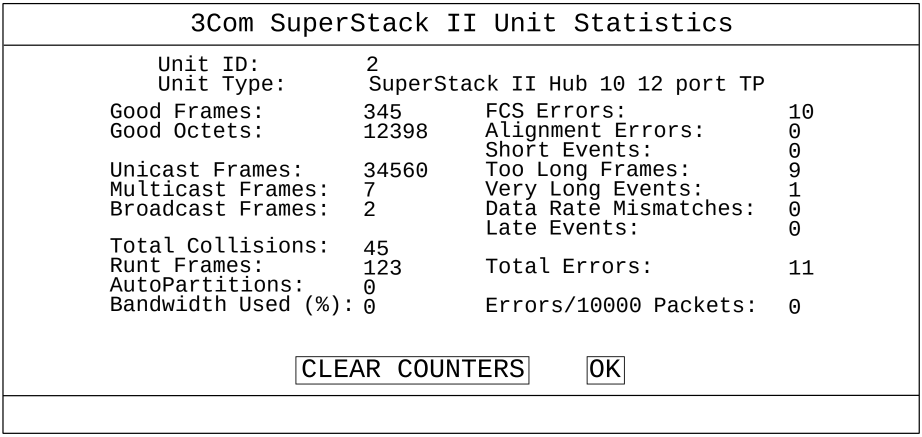
- Enabled - Unless both links have failed, the link is operational.
- Disabled - Both the main and standby ports are disabled.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the Repeater Management screen.

OK (Button) Select a resilient link pair, then move the cursor to this button and press [Return] to display the Port Resilience screen.

Unit Statistics

You access the Unit Statistics screen from the Repeater Management screen, by selecting management level *Unit* then actuating the STATISTICS button. The Unit Statistics screen is illustrated below. All the fields are read only. The statistics given are aggregates for all of the ports on the unit.



```
                3Com SuperStack II Unit Statistics

         Unit ID:         2
         Unit Type:       SuperStack II Hub 10 12 port TP
     Good Frames:        345       FCS Errors:              10
     Good Octets:        12398     Alignment Errors:        0
                                   Short Events:            0
     Unicast Frames:     34560     Too Long Frames:         9
     Multicast Frames:   7         Very Long Events:        1
     Broadcast Frames:   2         Data Rate Mismatches:    0
                                   Late Events:             0
     Total Collisions:   45
     Runt Frames:        123       Total Errors:            11
     AutoPartitions:     0
     Bandwidth Used (%): 0         Errors/10000 Packets:    0
```

Figure 3-19 Unit Statistics Screen

The screen is updated every 3 seconds. If the top limit of a counter (4294967295) is reached, the counter will *roll-over* (reset to zero automatically). After this event, the individual figures may give a false impression of network conditions if taken in isolation.

All the fields are read-only. Refer to Appendix D for a detailed description of the statistics fields.

Unit ID This field shows the identifying number of the unit you have selected from which to collect statistics.

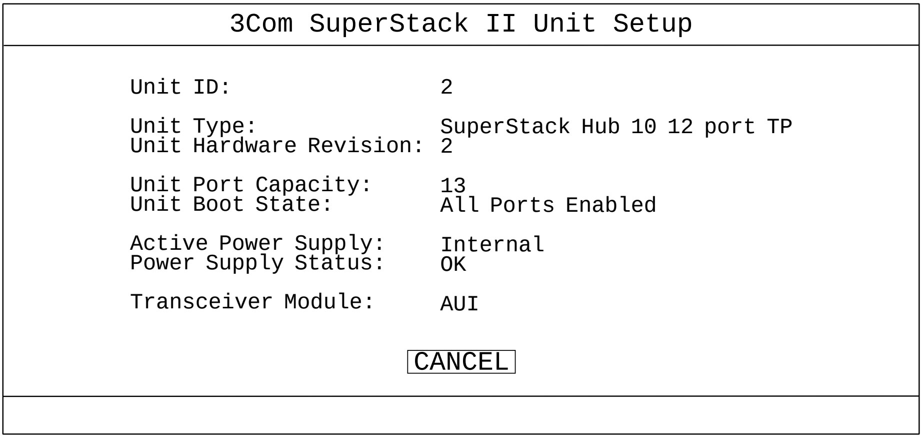
Unit Type This field identifies the type of unit you are managing.

CLEAR COUNTERS (Button) For users with an access level of manager or higher. Move the cursor to this button and press [Return] to reset all the unit statistics counters to zero. Clearing the unit's counters affects all users, and clears the counters for all the ports on this unit.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the Repeater Management screen without clearing the counters.

Unit Setup

You access the Unit Setup screen from the Repeater Management screen, by selecting management level *Unit* then actuating the SETUP button. The Unit Setup screen is illustrated below.



```
                 3Com SuperStack II Unit Setup

          Unit ID:                 2

          Unit Type:               SuperStack Hub 10 12 port TP
          Unit Hardware Revision:  2

          Unit Port Capacity:      13
          Unit Boot State:         All Ports Enabled

          Active Power Supply:     Internal
          Power Supply Status:     OK

          Transceiver Module:      AUI

                              CANCEL
```

Figure 3-20 Unit Setup Screen

The Unit Setup screen provides read only information. It shows how the unit has been set up, and the physical configuration of the unit at the time you display the screen. Changes made after the Unit Setup screen is displayed are not shown until the next occasion you display the screen.

Unit ID This field shows the identifier of the unit you have selected. This should be the same as that indicated by the Unit LED on the front of the chosen unit. The unit fitted with the Module is always unit 1.

Unit Type This field displays the product name or specification of the chosen unit.

Unit Hardware Revision This field indicates the hardware revision of the unit. You may need to quote this number to your supplier's technical support service in the event of a problem.

Unit Port Capacity This field indicates the maximum number of ports supported by the selected unit.

Unit Boot State This field indicates in what state the unit will boot up.

Only Hub 10 and FMS II units have a Disable on Boot switch.

The boot state is determined by the setting of the Disable on Boot switch, which is located behind the blanking plate or rear cover of the unit *(see Figure 2-1 on page 2-3).*

- All Ports Disabled - The unit boots up with all ports disabled (including AUI and transceiver module ports). For an existing unit, or replacement unit of the same type, the management facility then enables each port whose Port State in the Port Setup screen is currently set to *Enabled*.

At power up, there is a period of about 1 second during which the AUI and transceiver ports are not disabled.

- All Ports Enabled - The unit boots up with all ports enabled (including AUI and transceiver module ports). For an existing unit, or replacement unit of the same type, the management facility then disables each port whose Port State (in the Port Setup screen) is currently set to *Disabled*.

Active Power Supply This field indicates which power supply is currently active.

- Internal - the built-in power supply is active.
- External - The redundant backup power supply is active.

Only Hub 10 and FMS II units support an external, redundant backup power supply. You must NOT connect both the redundant backup power supply and mains power to a unit at the same time.

Power Supply Status This field indicates the status of the active power supply:

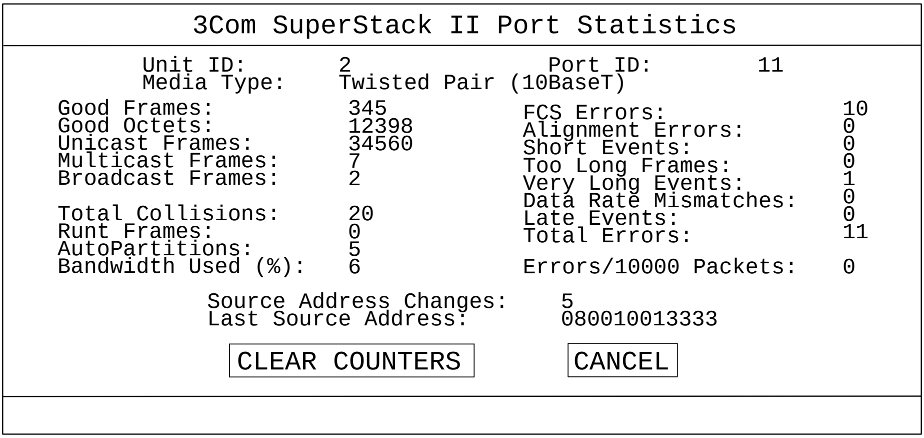
- OK - The power supply is functioning correctly.
- FAULT - Failure of part of the redundant backup power supply has been detected. Contact your supplier's technical support service.

Transceiver Module This field shows what type of module is fitted, if any, in the unit's transceiver module slot. Refer to the table in page 3-37 to identify the type of transceiver module fitted. If the unit has a shared AUI/transceiver port, this field shows *AUI* if no transceiver module is fitted. In other cases, *Not Fitted* is shown if no module is fitted in the slot.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the Repeater Management screen.

Port Statistics

You access the Port Statistics screen from the Repeater Management screen, by selecting management level *Port* then actuating the STATISTICS button. The Port Statistics screen is illustrated below.



```
                  3Com SuperStack II Port Statistics

           Unit ID:        2                Port ID:        11
           Media Type:     Twisted Pair (10BaseT)
    Good Frames:            345           FCS Errors:              10
    Good Octets:            12398         Alignment Errors:        0
    Unicast Frames:         34560         Short Events:            0
    Multicast Frames:       7             Too Long Frames:         0
    Broadcast Frames:       2             Very Long Events:        1
                                          Data Rate Mismatches:    0
    Total Collisions:       20            Late Events:             0
    Runt Frames:            0             Total Errors:            11
    AutoPartitions:         5
    Bandwidth Used (%):     6             Errors/10000 Packets:    0

                Source Address Changes:     5
                Last Source Address:        080010013333

              [CLEAR COUNTERS]         [CANCEL]
```

Figure 3-21 Port Statistics Screen

The screen is updated every 3 seconds. If the top limit of a counter (4294967295) is reached, the counter will *roll-over* (reset to zero automatically). After this event, the individual figures may give a false impression of network conditions if taken in isolation.

All the fields are read-only. Refer to Appendix D for a detailed description of the statistics fields.

Unit ID This field identifies the unit the port belongs to.

Port ID This field shows the number of the selected port.

Media Type This field indicates the media type of the port. See "Media Types" on page 3-37.

Source Address Changes This field shows the number of different source addresses that have been received at this port. If there is normally only one device connected to each port, it will allow you to monitor unauthorized devices connected to the network.

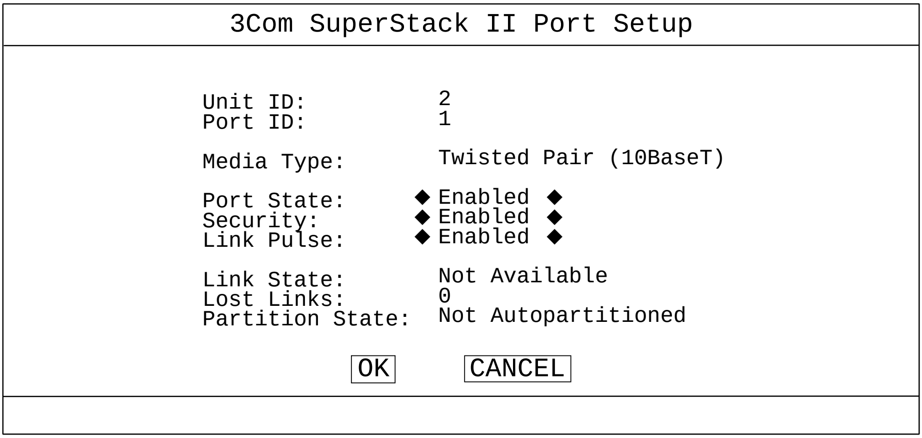
Last Source Address This field shows the source MAC address of the last frame received at this port.

CLEAR COUNTERS (Button) For users with an access level of manager or higher. Move the cursor to this button and press [Return] to reset all the port statistics counters to zero. Clearing the port's counters affects the statistics viewed by all users.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the Repeater Management screen.

Port Setup

You access the Port Setup screen from the Repeater Management screen, by selecting management level *Port* then actuating the SETUP button. The Port Setup screen allows you to configure a selected port. The screen is illustrated below.



```
                 3Com SuperStack II Port Setup


           Unit ID:             2
           Port ID:             1

           Media Type:          Twisted Pair (10BaseT)

           Port State:        ◆ Enabled ◆
           Security:          ◆ Enabled ◆
           Link Pulse:        ◆ Enabled ◆

           Link State:          Not Available
           Lost Links:          0
           Partition State:     Not Autopartitioned

                         [OK]      [CANCEL]
```

Figure 3-22 Port Setup Screen

The screen shows the following fields:

Unit ID (Read-only) This field shows the unit to which the port belongs.

Port ID (Read-only) This field shows the identifier of the port you selected to set up.

Media Type (Read-only) This field indicates the media type of the port. Use Table 3-4 to determine the media type.

Table 3-4 Media Types

Media Type	Description
AUI	Standard AUI (female) connection with no internal transceiver.
Modular Male AUI	Male AUI connection with internal transceiver.
Modular Female AUI	Female AUI connection with no internal transceiver.
Thin Coax (10Base2) †	Standard BNC Thin Ethernet connection.
Twisted Pair (10BASE-T) †	Twisted Pair RJ45 connection.
Fiber (10BaseFL) †	Fiber ST connection (10BaseFL / FOIRL).
Bridge †	Standard AUI (female) connection.
Not Fitted	No transceiver is installed.

† These media types may be prefaced by “Modluar” to indicate a tranceiver module is fitted.

Port State (Choice Field) Enabled / Disabled
The default state of a port is enabled. If you do not wish to use a port, set it to Disabled to prevent unauthorized access to the network.

You cannot enable or disable a port that is the main or standby port of a resilient link pair.

Security (Choice Field) Enabled/Disabled

All SuperSatck II Hub 10 units, all LinkBuilder FMS II 3C16665 and 3C16672 modules, and other LinkBuilder FMS II Modules with serial number prefixes of 0200 or greater, offer the more sophisticated security function detailed *below. Other units will display the Unauthorized Device Action field described below.*

This field provides access to the security features from the serial port in case you lock yourself out of in-band management.

When enabled, a default set of security features is applied to the unit much as described under Unauthorized Device Action below. The first address is learnt. Any different address will cause the port to be disconnected. The learnt address will receive traffic addressed to it, together with multicast and broadcast frames. Other traffic will be scrambled. If you use a 3Com Transcend management application, you have greater control over security, including support for multiple address per port.

With the designated Hub 10 units, you can set up secure, resilient pairs using a Transcend management application. Follow the instructions in the manual for that application.

Unauthorized Device Action (Choice Field)
Off / Report Only / Disconnect And Report
This field specifies the action to be taken when an unauthorized device is detected on the port. The management facility detects an unauthorized device when there is a change in the source address of frame or packets received by the port.

- Off - means no action will be taken.
- Report Only - means that a trap will be sent every 5 seconds to notify the remote network manager that an unauthorized device is accessing the port.
- Disconnect And Report - indicates that a trap will be sent to the network manager, and the port disabled. Refer to “Port Setup” on page 3-36 for details of how to re-enable the port.

Link Pulse (Choice Field) Enabled / Disabled
This field is applicable to 10BASE-T units only and will not be seen for other types of unit.

You can enable or disable the generation of link pulse signals for an individual port. In an 802.3 10BASE-T compliant network, leave this option at the default setting. If you are using non-compliant transceivers that do not use the link pulse signal, you will need to disable link pulse to enable the network to function correctly. Alternatively, you can replace non-compliant transceivers with 10BASE-T compliant transceivers, such as the ISOLAN TP Transceiver (3C16810).

Disabling generation of link pulses also disables detection of link pulses. In this case, repeater ports will assume that there is a connection and light the appropriate LEDs, even if there is no connection.
You cannot disable the link pulse for a port that is the main or standby port of a resilient link pair.

Link State (Read-only) This field shows the connection state of each port.

Table 3-5 Link States

Link State	Description
Other	The link state of this port cannot be recognized (for Coax and AUI ports.)
Unknown	The port is initializing. Its actual state is not yet known.
Available	The port is operating normally.
Not Available	The link has been lost (for 10BASE-T and 10BASE-FL ports).

Lost Links (Read-only) The number of times the link has been lost since the Module was last reset.

Partition State (Read-only) This field shows whether or not the port has autopartitioned. If it has, check the cabling at both the unit and any devices connected to that port.

Port Resilience

Resilient Links may be set up ONLY on Hub 10 and FMS II Units.

The Port Resilience screen allows you to create and delete a resilient link pair (main link and standby link), and to change the configuration of an existing resilient link pair.

There are three steps to setting up a resilient pair.

1 Disconnect the unit which is to provide the standby ports from the network. (We make this recommendation, even though it is possible to set up links whilst still connected, to avoid loops being formed accidently.)

2 Set up the pair from the Repeater Management screen. Select management level *Port*. Specify the unit and port of the main link. Actuate the RESILIENCE button to display the Port Resilience screen. Now you can specify the standby unit and port. See the field descriptions below.

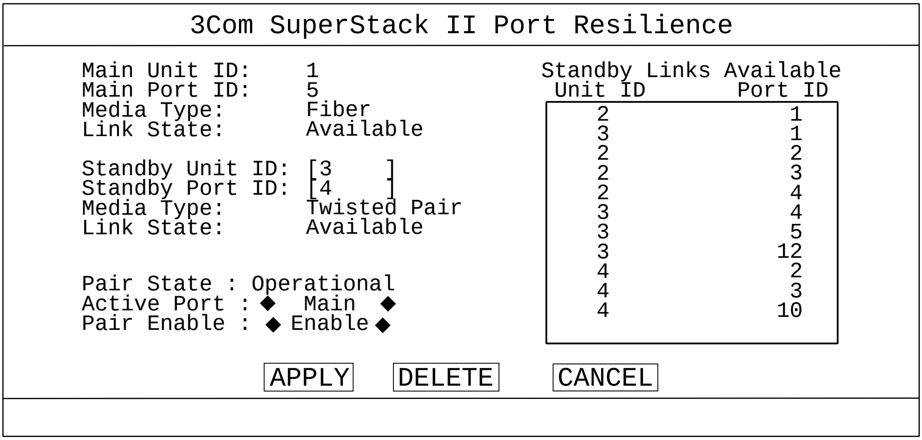
If the port you intended to use as standby is not shown in the list box, the unit which contains the port is not set for Disable on Boot. Change the switch position and reset the unit.

3 Reconnect the unit with the standby ports on it to the network.

To delete or change the configuration of a resilient link pair, do one of the following:

- From the Repeater Resilience screen, select the resilient link pair you want to configure, then actuate the OK button. The Port Resilience screen will be displayed.
- From the Repeater Management screen, select management level *Port*, then specify either the main port's or the standby port's unit and port ID. Actuate the RESILIENCE button to display the Port Resilience screen.

The Port Resilience screen is illustrated below.



```
                3Com SuperStack II Port Resilience

Main Unit ID:     1                 Standby Links Available
Main Port ID:     5                  Unit ID        Port ID
Media Type:       Fiber                 2              1
Link State:       Available             3              1
                                        2              2
Standby Unit ID: [3     ]               2              3
Standby Port ID: [4     ]               2              4
Media Type:       Twisted Pair          3              4
Link State:       Available             3              5
                                        3             12
Pair State : Operational                4              2
Active Port : ◆  Main  ◆                4              3
Pair Enable : ◆ Enable ◆                4             10

          APPLY    DELETE     CANCEL
```

Figure 3-23 Port Resilience Screen

Rules for setting up resilient links

A resilient pair cannot be set up through the VT100 screens if one or either of the ports is a secure port.

- You can set up a resilient link pair to use ports on the same unit, or on different units in the stack to prevent the loss of both links should a single unit fail. This applies to fiber and twisted pair transceiver module ports, but NOT to AUI ports with external transceivers fitted.
- The resilient link pair can be set up only on fiber or twisted pair media types, although the main and standby links can be both media types.
- The standby port must be configured so that it is Disabled on Boot. This ensures that a loop will not be created when the unit boots up.

This means that a standby port can be configured only on a Hub 10 or an FMS II unit, and that the Disable on Boot switch (see Figure 2-1 on page 2-3) on the unit must be set to 'Disable'. Refer to the unit's user manual for instructions on how to set the switch.

- The resilient link pair must only be defined at one end of the link.
- A resilient link pair can only be set up if neither of the ports already form part of another resilient link.

- The number of resilient links per stack must not exceed 16.

Resilience works by monitoring the fiber receive idle signal or the 10BASE-T link Test Pulse, to determine whether or not the main link is operational. If a loss of link is detected, the main port is disabled and the standby port becomes the active port.

If the main link becomes operational again, the management facility does not automatically make the main port the active port. You can achieve this manually by setting the Active Port field to *Main*.

The fields in the Port Resilience screen are:

Main Unit ID (Read-only) This field shows the identifier of the unit that the main port belongs to.

Main Port ID (Read-only) This field shows the identifier of the main port.

Media Type (Read-only) This field shows the media type for the main port. Refer to Table 3-4 on page 3-37.

Link State (Read-only) This field shows the connection state of the main port. Refer to Table 3-5 on page 3-39 for the different states.

Standby Unit ID (Text Field) This field shows the unit identifier of the unit that the standby port belongs to. You can either enter the identifier of the chosen standby unit, or select a standby unit and port from the list box.

Standby Port ID (Text Field) This field shows the identifier of the standby port. You can either enter the identifier of the chosen standby port, or select a standby unit and port from the list box.

The standby port must be configured so that it is Disabled on Boot, otherwise it will not be listed as a possible standby link. This means that the Disable on Boot switch of the Hub 10 unit (see Figure 2-1 on page 2-3) with the standby port must be set to 'Disable'. Refer to the unit's user manual for instructions on how to set the switch.

Media Type (Read-only) This field shows the media type for the standby port. Refer to Table 3-4 on page 3-37 for the different media types.

Link State (Read-only) This field shows the connection state of the standby port. Refer to Table 3-5 on page 3-39 for the different states.

Pair State (Read only) This field shows the state of the currently active selected resilient pair, if any. Possible values are:

- Active - The link pair is enabled, and either the main port or the standby port is capable of carrying traffic.
- Not in use - The link pair is disabled.
- Both Failed - Although the link pair is correctly configured, both links have failed.
- Invalid - The state of the repeater has changed since the link pair was configured, and the link pair now does not conform to the resilient link rules (see earlier in this section). An example is where the Disable on Boot switch of the unit with the standby port has been changed to Enable.

Active Port (Choice Field) Main/Standby
Select the port you want to carry the traffic.

Pair Enable (Choice Field) Enabled/Disabled
Use this field to enable or disable the resilient link pair. If you disable a link pair, both the main and standby ports will be disabled.

Standby Links Available (List Box) The list box shows the Unit ID and Port ID of the possible standby links for the selected main link. These are all the Disable on Boot ports that are not already part of a resilient link pair. To select a standby link, move the cursor to the list box and use the arrow keys until the desired link is highlighted, then press [Return]. The unit and port identifiers of the selected unit will be copied into the Standby Unit ID and Standby Port ID fields.

APPLY (Button) Move the cursor to this button and press [Return] to configure the resilient link pair. When the link is configured, you are returned to the previous screen.

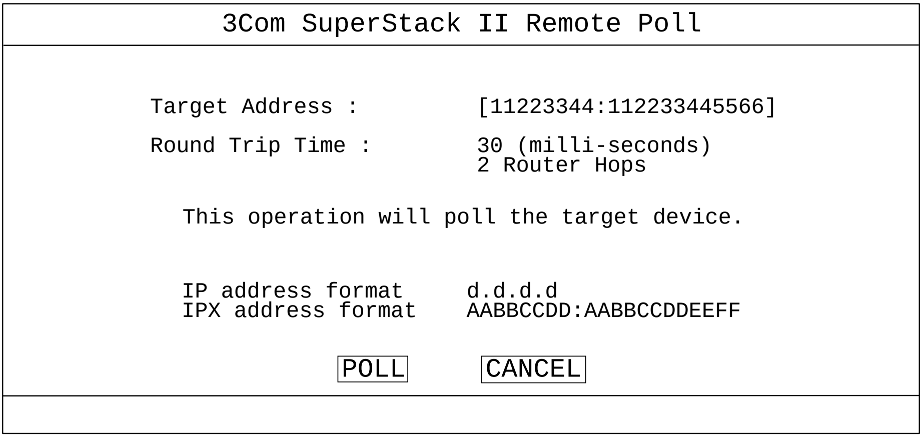
When you configure a resilient link pair, the management facility will automatically enable Link Pulse generation (see "Port Setup" on page 3-36) for both ports. If you subsequently delete the resilient link pair, Link Pulse generation remains enabled.

DELETE (Button) Move the cursor to this button and press [Return] to delete the resilient link pair specified by the Main Unit ID, Main Port ID, Standby Unit ID and Standby Port ID fields. You will be asked to press [Return] again for confirmation.

CANCEL (Button) Move the cursor to this button and press [Return] to go back to the previous screen (either the Repeater Management screen or the Repeater Resilience screen).

Remote Poll

The Remote Poll screen allows you to see if a remote device is responding, by sending a message forcing a response from the target device. This will determine if there is a path or a congested path between this device and other devices on the network. To display the screen, actuate the REMOTE POLL button on the Main Menu screen (only available to users with *manager* access level or higher.)



```
                3Com SuperStack II Remote Poll


         Target Address :         [11223344:112233445566]

         Round Trip Time :        30 (milli-seconds)
                                  2 Router Hops

           This operation will poll the target device.


           IP address format     d.d.d.d
           IPX address format    AABBCCDD:AABBCCDDEEFF

                         POLL        CANCEL
```

Figure 3-24 Remote Poll Screen

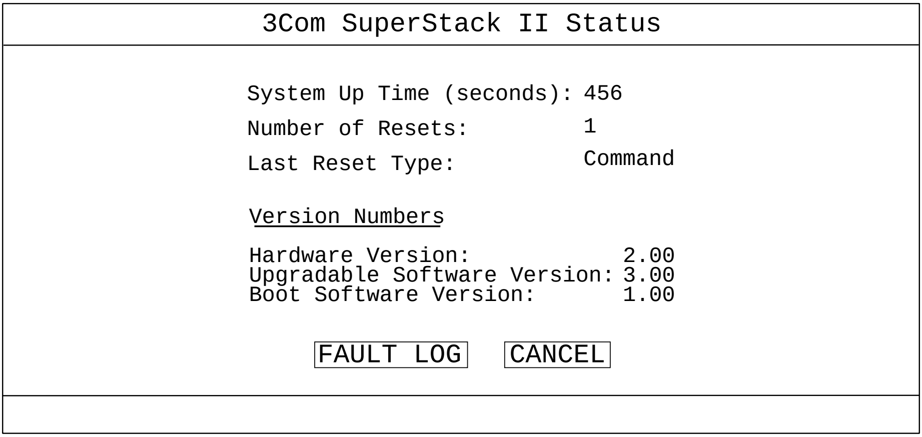
Target Address (Text Field) Enter the IP or IPX address of the device to poll.

Round Trip Time (Read-only) This is the interval in milliseconds between the time the last frame was sent to the target device and the time a response was received by the Module. If there is no response within a few seconds, *no reply* is shown. Also displayed will be the number of router hops and, if set, the time-to-live for the frame.

The Module can be configured to automatically poll several devices at regular intervals, and report back to a management station if there is no response. This facility is only available through SNMP management.

Status

The Status screen provides read-only information about the Module. To display the screen, select the STATUS button on the Main Menu screen.



```
3Com SuperStack II Status

System Up Time (seconds): 456
Number of Resets:         1
Last Reset Type:          Command

Version Numbers

Hardware Version:             2.00
Upgradable Software Version: 3.00
Boot Software Version:        1.00
```

Figure 3-25 Status Screen

System Up Time (seconds) This field indicates how long the unit has been running since the last reset. See "Reset" on page 3-48 for a description of resetting the unit.

Number of Resets This field shows the total number of system resets since the Module was first installed, or initialized. This information may be useful to your technical support representative in the event of problems.

Last Reset Type This field indicates the cause of the last reset. This information may be useful to your technical support representative in the event of problems.

Hardware Version This is the hardware version of the Module installed in the unit. Please make a note of this number in case you ever need to contact your technical support representative.

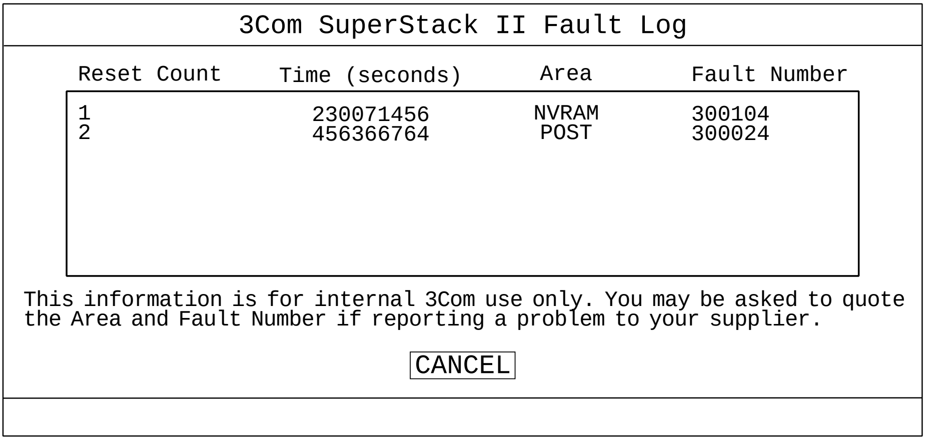
Upgradeable Software Version This is the version number of the software image stored in the Flash EPROM. Please make a note of this number in case you ever need to contact your technical support representative. The version number will be automatically updated when you download new software.

Boot Software Version This is the version number of software stored in the Boot PROMs on the Module. Please make a note of this number in case you ever need to contact your technical support representative.

Fault Log (Button) Select to view the fault log.

Fault Log

The Fault Log screen displays read-only information about the log, which is updated whenever an abnormal condition is detected.



```
                  3Com SuperStack II Fault Log

      Reset Count      Time (seconds)       Area          Fault Number
      1                  230071456          NVRAM         300104
      2                  456366764          POST          300024

   This information is for internal 3Com use only. You may be asked to quote
   the Area and Fault Number if reporting a problem to your supplier.
```

Figure 3-26 Fault Log Screen

Reset Count This field displays the number of resets recorded at the time of the fault.

Time (seconds) This field shows the time since the last reset that the fault occurred.

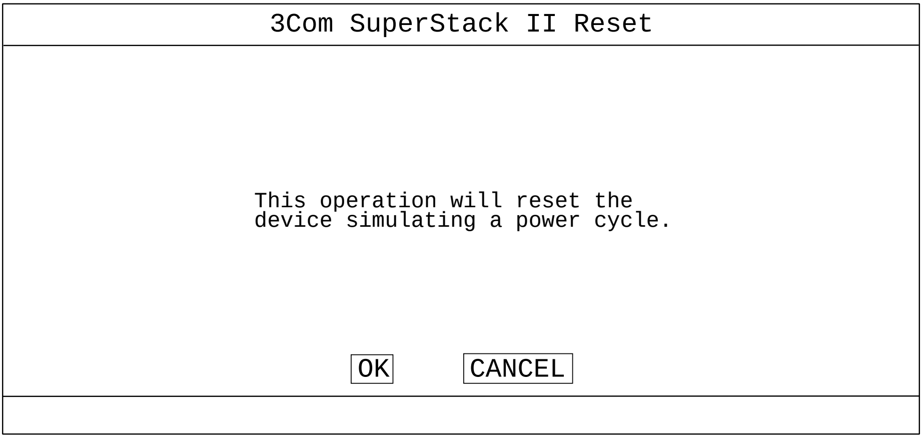
Area This field identifies the hardware or software that generated the fault. Make a note of this information, which will be useful to your technical support representative in resolving the fault.

Fault Number The hexadecimal number in this field provides an indication of the type of fault. *It is for 3Com internal use only*. Record any information on this screen and contact your Technical Support service for advice.

Reset

If you suspect that the stack is not functioning correctly in the way you have configured it, you can reset the entire stack from the Reset screen. This has the same effect as pressing the Reset button on the rear of the Module.

To display the screen, actuate the RESET button on the Main Menu screen. (This is only available to users with *manager* access level or higher.)



3Com SuperStack II Reset

```
This operation will reset the
device simulating a power cycle.
```

Figure 3-27 Reset Screen

Resetting the stack in this way is similar to powering off and on the unit containing the Module. None of the setup information will be lost.

CAUTION: *Performing a reset may cause some of the data being transmitted onto the network to be lost.*

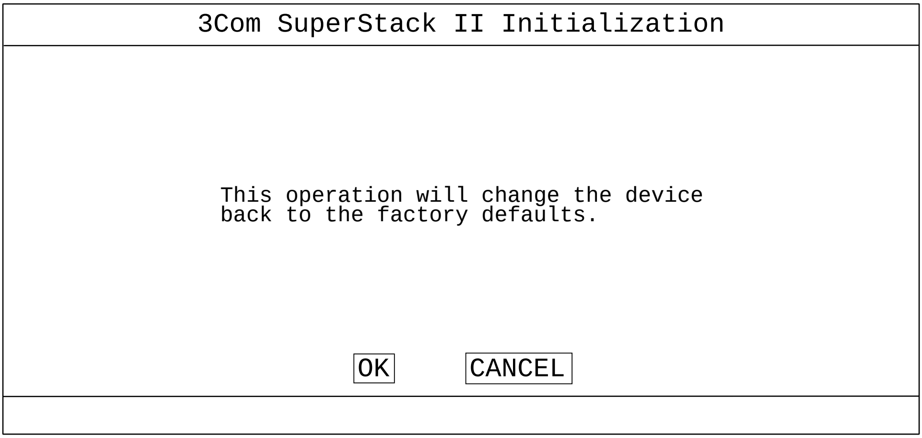
Select the OK button to perform the reset.

Initialization

This operation is only available to users with *security* access level. The initialization operation performs a reset as described in “Reset” on page 3-48, and in addition returns the NVRAM to its initial values. You should only initialize the stack if:

- The configuration of the stack no longer suits your network.
- Other troubleshooting efforts have failed.

To display the Initialization screen, actuate the INITIALIZE button on the Main Menu screen.



```
                 3Com SuperStack II Initialization

              This operation will change the device
              back to the factory defaults.
```

Figure 3-28 Initialization Screen

Select OK to perform the initialization.

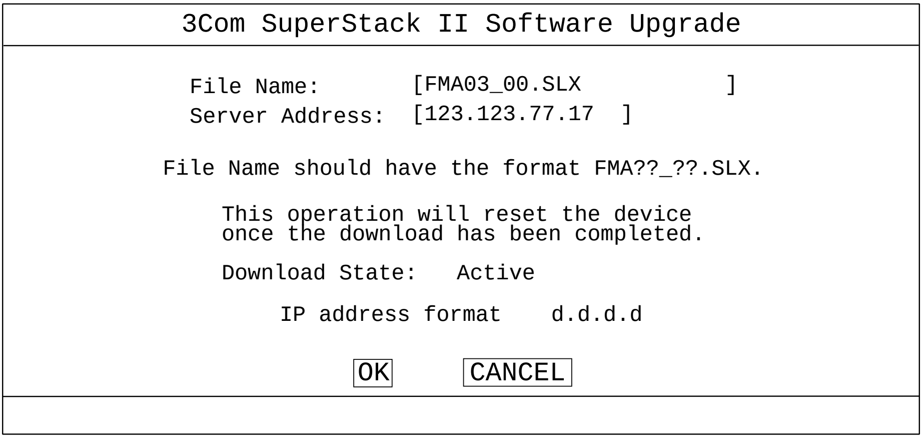
CAUTION: *Use this operation with great care. The unit configuration is cleared from memory and cannot be recovered. All user information (except the IP parameters) will be lost and only the default users will be available. All ports will be set to their hardware default values, which may make unused disabled ports enabled and thus available to users. This may also cause a loop through the resilient links.*

Software Upgrade

This option is only available to users with *security* access level.

When 3Com issues a new version of the Module SmartAgent software, you can obtain the software image from 3Com bulletin board services (see Appendix B).

You use the Software Upgrade screen to download software images. To display the screen, actuate the SOFTWARE UPGRADE button on the Main Menu screen.



```
            3Com SuperStack II Software Upgrade

      File Name:        [FMA03_00.SLX             ]
      Server Address:   [123.123.77.17  ]

    File Name should have the format FMA??_??.SLX.

         This operation will reset the device
         once the download has been completed.

         Download State:   Active

              IP address format    d.d.d.d

                     OK        CANCEL
```

Figure 3-29 Software Upgrade Screen

The filename you will download will reflect the management product you have installed.

The protocol used for downloading is TFTP running over UDP/IP or IPX and will only work over the network, not via the serial port. To perform the download, a remote TFTP server must be set up.

File Name (Text Field) Enter the name of the file that contains the software image to be downloaded to the Module. You will be prompted with a file format appropriate to the Module. This will be FMAxx_xxx.slx for the Management Module or FMRxx_xx.slx for the Advanced RMON Module. You will not be allowed to download the wrong image. You must place the image file where it is accessible to the TFTP load request. Check with your system administrator if you are unsure where to place the image file.

You may wish to download the file from another directory. If so, you must give the full path to the file and the filename, using a maximum of 30 characters.

Server Address (Text Field) Enter the IP or IPX address of the device where the software file containing the image of the Module facility can be found.

OK (Button) Select this button to start the software download. When the download is being performed, the MGMT LED will flash green and the screen will be locked. When the download is complete, the Module will be reset.

A TECHNICAL INFORMATION, CABLE PIN-OUTS AND PROTOCOLS

Standards

The SuperStack II Hub 10 Management Module and the Advanced RMON Module are designed to meet the following standards:

Safety

UL1950
EN 60950
CSA 22.2 #950
ECMA 97

EMC

CSA C108.8 - M1983 Class A
FCC Part 15 Class A
IEC 801 (parts 2-5)
EN55022 Class B
EN50082-1

Environmental

IEC 68 to 3Com Schedule.

Operational 0°C to 50°C.

BABT Approval

For UK Users only.
The SuperStack II Hub 10 units, fitted with a Management Module or Adavnced RMON Module, are covered by Oftel General Approval, NS/G/12345/J/100003, for indirect connection to a public telecommunications system. This can be achieved using the serial port and an approved modem.

Electrical

These figures apply to the device listed when fitted with a SuperStack II Hub 10 Management Module or SuperStack II Hub 10 Advanced RMON Module.

Power Consumption

3C16665A	46 VA
3C16670A	28 VA
3C16671A	34 VA
3C16672A	34 VA

Power Dissipation

3C16665A	156 BTU/hr
3C16670A	94 BTU/hr
3C16671A	115 BTU/hr
3C16672A	115 BTU/hr

Processor and Memory

Management Module

Flash EPROM	512 Kbytes
RAM	512 Kbytes
Processor	10MHz 68000

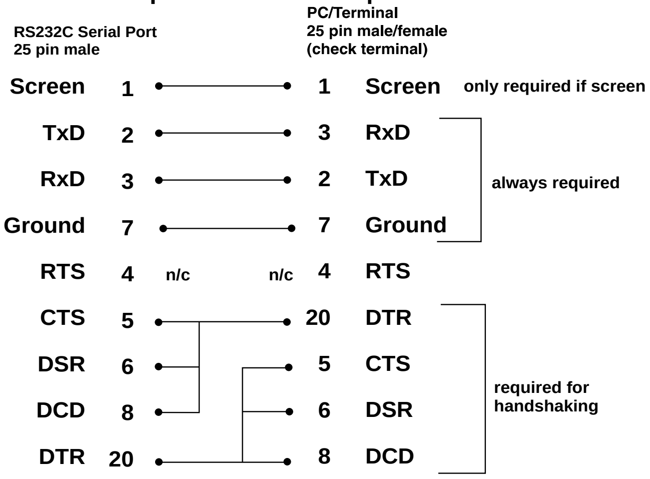
Advanced RMON Module

Flash EPROM	512Kbytes
RAM	4Mbytes
Processor	20MHz 68000

Cable Pin-Outs

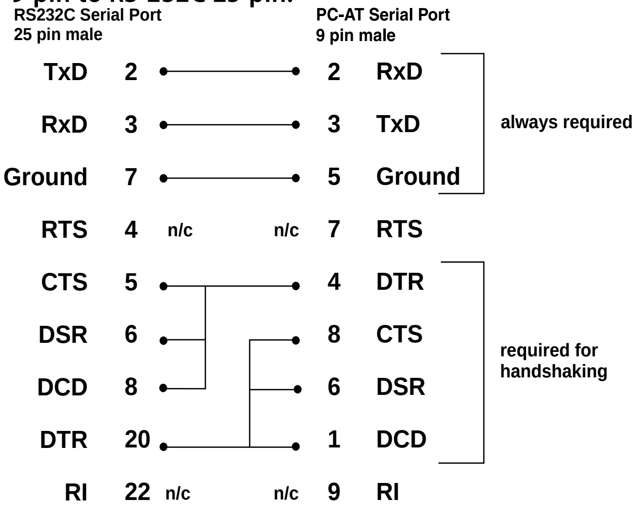
This section shows the pin-outs for the Management Terminal cable used to connect a terminal, PC or modem to the serial port (RS-232C management port).

Null Modem Cable
RS-232C 25 pin to RS-232C 25 pin.



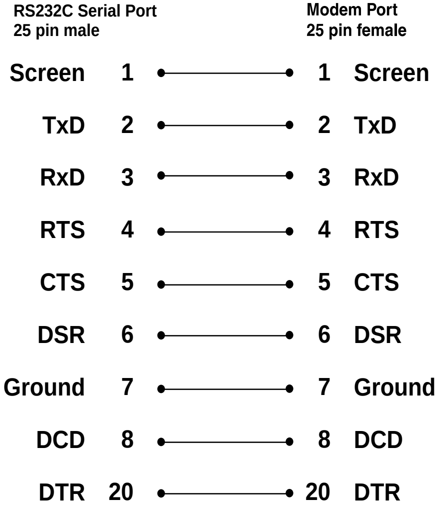
PC-AT Serial Cable

9 pin to RS-232C 25 pin.



Modem Cable

RS-232C 25 pin to RS-232C 25 pin.



Protocol Addresses

IPX Addresses

If you are using the IPX protocol, the Module will be allocated an IPX address automatically by the local IPX router or NetWare File Server. This happens approximately 60 seconds after the unit is powered up for the first time. You should never need to change the allocated address.

IP Addresses

IP (Internet Protocol) addresses have the format n.n.n.n where n is a decimal number between 0 and 255. An example IP address is: 192.168.100.120

IP addresses are made up of two parts:

- The first part (192.168 in the example) identifies the network on which the device resides. Network addresses are assigned by three organizations. Depending on your location, each organization assigns a globally unique network number to each network that wishes to connect to the Internet.
- The second part (100.120 in the example) identifies the device within the network. Assigning unique device numbers is your organization's responsibility.

If you are unsure of the IP addresses allocated to you, consult your network administrator. If you do not have an Internet address, see “Obtaining a Network Number” on page A-6.

If you are the manager of a network that has no connections to the outside world, you may not be aware of the network address. If you are not using the IP protocol for anything other than network management, you may use arbitrary addresses. We suggest you use addresses in the series 192.168.100.Y, where Y is a number between 1 and 254. Use 192.168.101.Y for the SLIP address (192.168.101.1 is the default setting) . Remember that no two devices on a network may have the same address. If you later connect to the outside world, you must change all the arbitrary IP and SLIP addresses, to comply with those you have been allocated by Network Information Center (NIC). If you do not do this, your outside communications will not operate.

A subnet mask is a filtering system for IP and SLIP addresses. If you are unsure about what mask to use, we suggest you use a general mask, 255.255.255.0, to tie in with the advice above.

Obtaining a Network Number

There are three organizations responsible for allocating network numbers. The details are correct at the time of printing, but they may change.

USA - InterNIC, Network Solutions

Attention:	InterNIC Registration Services 505 Huntmar Park Drive Herndon VA 22070
Telephone:	1-800-444-4345 (Toll Free) 1-619-455-4600 1-703-742-4777

You can also send e-mail to the addresses listed below.

hostmaster@rs.internic.net	(host, domain, network changes and updates)
action@rs.internic.net	(computer operations)
mailserv@rs.internic.net	(automatic mail service)
info@internic.net	(automatic mail service for general enquiries)
refdesk@is.internic.net	(enquiries not handled by the services above)

Europe - RIPE

Attention:	RIPE NCC Kruislaan 409 NL-1098 SJ Amsterdam The Netherlands

Telephone	+31 20 592 5065
Fax:	+31 20 592 5090
e-mail:	ncc@ripe.net

Asia Pacific Network Information Centre (APNIC-DOM)

Attention:	Asia Pacific Network Information Centre (APNIC-DOM) c/o Computer Centre, University of Tokyo 2-11-16 Yayoi Bunkyo-ku, Tokyo 113 Japan
Admin. Contact:	Nakayama, Masaya (MN89)
Telephone:	+81 3 3812 2111 ext2720
e-mail:	nakayama@nic.ad.jp
Technical Contact:	Conrad, David (DC396)
Telephone:	+81 3 3580 3781 or +81 3 3580 3784
Fax:	+81 3 3580 3782
e-mail:	davidc@apnic.net

B TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

On-line Technical Services

3Com offers worldwide product support seven days a week, 24 hours a day, through the following on-line systems:

- 3Com Bulletin Board Service (3ComBBS)
- World Wide Web site
- ThreeComForum on CompuServe®
- 3ComFacts^{SM} automated fax service

3Com Bulletin Board Service

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem or ISDN seven days a week, 24 hours a day.

Access by Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	(61) (2) 9955 2073
France	up to 14400 bps	(33) (1) 69 86 69 54
Germany	up to 9600 bps up to 9600 bps	(49) (89) 627 32 188 (49) (89) 627 32 189
Hong Kong	up to 14400 bps	(852) 537 5608

Country	Data Rate	Telephone Number
Italy (fee required)	up to 14400 bps	(39) (2) 273 00680
Japan	up to 14400 bps	(81) (3) 3345 7266
Singapore	up to 14400 bps	(65) 534 5693
Taiwan	up to 14400 bps	(886) (2) 377 5838
U.K.	up to 28800 bps	(44) (1442) 278278
U.S.	up to 28800 bps	(1) (408) 980 8204

Access by ISDN

ISDN users can dial-in to 3ComBBS using a digital modem for fast access up to 56 Kbps. To access 3ComBBS using ISDN, dial the following number:

(408) 654-2703

World Wide Web Site

Access the latest networking information on 3Com's World Wide Web site by entering our URL into your Internet browser:

`http://www.3Com.com/`

This service features news and information about 3Com products, customer service and support, 3Com's latest news releases, selected articles from 3TECH™ (3Com's award-winning technical journal), and more.

ThreeComForum on CompuServe

ThreeComForum is a CompuServe-based service containing patches, software, drivers, and technical articles about all 3Com products, as well as an interactive forum for technical questions. To use ThreeComForum, you need a CompuServe account.

To use ThreeComForum:

1. Log on to CompuServe.
2. Enter **`go threecom`** .
3. Press [Return] to see the Ask3Com main menu.

3ComFacts Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, seven days a week.

Call 3ComFacts using your touch-tone telephone. International access numbers are:

Country	Fax Number
Hong Kong	(852) 2537 5610
U.K.	(44) (1442) 278279
U.S.	(1) (408) 727 7021

Local access numbers are available within the following countries:

Country	Fax Number	Country	Fax Number
Australia	800 123853	Netherlands	06 0228049
Belgium	0800 71279	Norway	800 11062
Denmark	800 17319	Portugal	0505 442607
Finland	98 001 4444	Russia (Moscow only)	956 0815
France	05 90 81 58	Spain	900 964445
Germany	0130 8180 63	Sweden	020 792954
Italy	1678 99085	U.K.	0800 626403

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages

- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

In the U.S. and Canada, call **(800) 876-3266** for customer service.

If you are outside the U.S. and Canada, contact your local 3Com sales office to find your authorized service provider:

Country	Telephone Number
Australia (Sydney)	(61) (2) 959 3020
(Melbourne)	(61) (3) 653 9515
Belgium*	0800 71429
Brazil	(55) (11) 546 0869
Canada	(416) 498 3266
Denmark*	800 17309
Finland*	0800 113153
France*	05 917959
Germany*	0130 821502
Hong Kong	(852) 868 9111
Ireland*	1 800 553117
Italy*	1678 79489
Japan	(81) (3) 3345 7251
Mexico	(525) 531 0591
Netherlands*	06 0227788
Norway*	800 13376
Singapore	(65) 538 9368
South Africa	(27) (11) 803 7404
Spain*	(34) (1) 3831700
Sweden*	(46) (8) 632 91 00
Taiwan	(886) (2) 577 4352
United Arab Emirates	(971) (4) 349049
U.K.*	0800 966197
U.S.	(1) (408) 492 1790

* These numbers are toll-free

Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S. and Canada	(800) 876 3266, option 2	(408) 764 7120
Europe	31 30 60 29900, option 5	(44) (1442) 275822
Outside Europe, U.S. and Canada	(1) (408) 492 1790	(1) (408) 764 7290

C TROUBLESHOOTING

In the main chapters, we have indicated where problems can occur when using the management facility. This appendix collects together this troubleshooting information. It will help you to determine the cause of a problem, should one arise, and to correct the problem. It lists symptoms that may appear, and suggests what actions to take to track down and resolve the problem.

The initial Main Banner screen will not display.

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

For serial port access, check you have performed the wake-up procedure correctly, by pressing [Return][Return].

Check the settings on your terminal or emulator. The parity must set to ’none’, the stop bit’1’ and the character size ’8’. The management facility's autoconfiguration works only with speeds from 1200 to 9600 baud.

Possibly, autoconfiguration is disabled.

If you still cannot access the device, perform a reset by pressing the Reset switch at the rear of the Module once. Now check the MGMT LED on the front of the management unit (unit 1). The LED should be green. If it is red, and remains red after you perform a reset a number of times, contact your supplier.

If the MGMT LED is off, there is no Module installed, or the unit cannot correctly identify the installed module. Check that the connector cables are secure, and that you have installed the module correctly as described in Chapter 2.

If you still cannot resolve the problem, the Module itself may be faulty. Contact your supplier.

Screens are incorrectly displayed.

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

Check the settings on your terminal or emulator. The parity must set to 'none', the stop bit '1' and the character size '8'. The management facility's autoconfiguration works only with speeds from 1200 to 9600 baud.

The SNMP manager cannot access the device.

Check the device's IP address, subnet mask and default router are correctly configured (see "Setup" on page 3-10) and the device has been reset (see "Reset" on page 3-48). Check that the device's IP address is correctly recorded by the SNMP manager (refer to the user manual for the manager).

The Telnet workstation cannot access the device.

Check the device's IP address, subnet mask and default router are correctly configured (see "Setup" on page 3-10) and the device has been reset (see "Reset" on page 3-48). Ensure that you enter the IP address correctly when invoking the Telnet facility.

Traps are not received by the SNMP manager.

Check the SNMP manager's IP address and the community string is correctly configured (see "Trap Setup" on page 3-13).

The SNMP manager or Telnet workstation can no longer access the device.

Check that Remote Telnet access or Community-SNMP access is enabled (see "Local Security" on page 3-18).

Check that the port through which you are trying to access the device has not been disabled (see "Port Setup" on page 3-36). If it is enabled, check the connections and network cabling at the port.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

Possibly there is a network problem preventing you accessing the device over the network. Try accessing the device through the serial port.

Try resetting the device by pressing the reset switch.

You forget your password and cannot log in.

If you are not one of the default users (monitor, manager or security), another user having *security* access level can log in, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having *security* access level can log in and initialize the device, as described in "Initialization" on page 3-49. This will return all configuration information, including passwords, to the initial values.

In the case where no-one knows a password for a security level user, contact your supplier.

D STATISTICS

This appendix lists the terms that are used in the Repeater Statistics, Unit Statistics and Port Statistics screens. There are suggestions for courses of action to take, if required. In general, if repeater statistics indicate a problem, try to isolate the source of the problem by examining unit and then port statistics.

Alignment Errors An alignment error occurs if the last byte of the frame is not received whole. The number of alignment errors should be a very small percentage of the total data traffic.

Alignment errors are likely to be caused by a fault at the transmitting device. Check the transceiver or adapter card of the device connected to the port that is the source of the problem. If the card appears to be operating correctly, check the cable and cable connections for breaks or damage.

Auto Partitions The number of times the port or ports have automatically partitioned. Autopartitioning occurs when excessive (more than 64) consecutive collisions occur at a port.

Autopartitioned ports are automatically reconnected when the fault is rectified. Frequent partitions can indicate that there is a problem in the cabling between two units or a unit and an attached device. It can also indicate that a device is faulty. Check the cabling at both the stack and the devices connected to it.

Bandwidth Used (%) The percentage bandwidth used. This statistic gives an indication of the general traffic level of the network.

Broadcast Frames The total number of broadcast frames seen at the repeater, unit or port. Broadcast frames are frames that are addressed to all MAC addresses (that is, all devices) on the network. The total number of broadcast frames will normally be a small percentage of the value seen for unicast frames. A high level of broadcast frames can adversely affect network performance.

Data Rate Mismatches The number of frames received by the repeater, unit or port whose timing was outside the permitted frequency range. This may indicate non-compliant or faulty devices on your network.

Errors/10000 Packets The number of total errors per 10,000 packets received by the repeater, unit or port. This statistic gives an indication of the general health of the network. A sudden significant change in the value of this parameter usually indicates a problem developing.

FCS Errors Frame Check Sequence (FCS) errors indicate that frames of data are being corrupted. FCS errors are counted when incoming frames fail the Cyclic Redundancy Check (CRC) test. The number of FCS errors should be a very small percentage of the total data traffic.

Check the transceiver or adapter card of the device connected to the port that is the source of the problem. If the card appears to be operating correctly, check the cable and cable connections for breaks or damage. Occasionally the problem may be caused by interference from other cables or machinery.

Good Frames This is the total number of frames with no errors seen by the repeater, unit or port. Examining this statistic regularly can help you monitor your network's overall performance. Look for unusual increases in traffic rate. This may indicate a potential problem, or help you decide if a bridge is required on your network.

Good Octets This field shows the total number of octets (bytes) received as part of good frames seen at the repeater, unit or port. The total includes the header, data and CRC octets of each frame. The Good Octets value allows you to calculate the throughput, in terms of bytes per second, and the average frame size on your network.

Late Events A Late Event is an out of window collision, which may occur if you have an 802.3 LAN that exceeds the maximum size as defined by IEEE. A Late Event is also counted as a collision.

Multicast Frames This is the total number of multicast frames seen at the repeater, hub or port. A multicast frame is one that is addressed to a group of MAC addresses (that is, several devices) on the network. The total number of multicast frames will normally be a small percentage of the value seen for unicast frames.

A high level of multicast frames can adversely affect network performance.

Runt Frames Runt frames are frames that are smaller than the minimum frame size defined for 802.3 frames, but longer than Short Events. Runt frames may occur as the result of collisions, and will be propagated around the network. This is a normal part of CSMA/CD operation and is not an error.

Short Events Short Events are smaller than runt frames and are errors. They may indicate externally generated noise causing problems on the network.

Check the cable routing and re-route any cabling which may be affected by external noise sources.

Too Long Frames Too Long Frames are frames that exceed the maximum size for 802.3 frames (1518 octets).

If you see a high number of such frames you will need to isolate the source of these frames and examine the transceiver or adapter card at the device. However, some network protocols cause these frames.

Total Collisions Collisions are a normal part of 802.3 operation and occur if two devices attempt to transmit at the same time.

A sudden sustained increase in the number of collisions may indicate a problem with a device or cabling on the network, particularly if this is not accompanied by a general increase in traffic.

Total Errors This field should be a small proportion of the Good Frames figure. It is the sum of the following errors seen in the unit:

FCS Errors, Alignment Errors, Short Events, Too Long Frames, Very Long Events, Data Rate Mismatches, Late Events.

Transmit Collisions Transmit collisions are collisions that take place at the stack, as opposed to those that take place on the network and are detected at the stack. Collisions are a normal part of 802.3 operation, and are not errors. Transmit collisions form part of the Total Collisions figure.

Unicast Frames This is the total number of frames addressed to a single MAC address (that is, a single device) seen at the repeater, unit or port.

Very Long Events A very long event is an event that will cause Jabber Lock Up protection to operate. This statistic shows how many times the repeater has had to protect against jabber seen at a port.

Isolate the source of very long events and check that the transceiver or adapter card in the device is operating correctly.

E RMON AND ADVANCED MANAGEMENT

What is RMON?

Transcend SmartAgent RMON provides a mechanism for remote monitoring and analysis of a Local Area Network. RMON is the common abbreviation for the Remote Monitoring MIB as defined by the IETF in documents RFC 1271 and RFC 1757. A typical RMON system consists of two components:

- **The Probe** - Connects to a LAN segment, examines all the LAN traffic on that segment and keeps a summary of statistics (including historical data) in its local memory.
- **The Management Console -** Communicates with the Probe and collects the summarized data from it. The console does not have to be on the same network as the probe and can manage the probe by either in-band (SNMP) or out-of-band connections.

The IETF defines the following groups of information supplied by ethernet RMON probes.

Statistics	Total LAN statistics
History	Time-based statistics for trend analysis
Alarms	Triggered when statistics reach pre-defined thresholds
Events	Reporting mechanism for alarms
Hosts	Statistics stored by station MAC Address
HostTopN	Stations ranked by traffic or errors
Matrix	Traffic Matrix (who is talking to whom)
Filter	Packet selection mechanism
Packet Capture	Allows traces of packets against pre-defined filters

Benefits of RMON

Traditional network management involves a network management console polling network devices (e.g. hubs, bridges, routers) at regular intervals to gather statistics and identify problems or trends. As network sizes and traffic levels grow, however, this approach places a strain on the network management console which may not be able to keep up. It also generates a lot of network management traffic which itself adds to the problems.

An RMON probe, on the other hand, autonomously looks at the network on behalf of the network management console without in any way affecting the characteristics and performance of the network. An important characteristic of RMON is that it reports by exception. The traditional approach involves the constant interrogation of network devices just to find out if the network is within its normal operating conditions. RMON informs the network management console directly when the network has entered an abnormal state. The console can then use more information from the probe (such as history information and packet capture) to perform additional diagnoses.

3Com Transcend RMON SmartAgents

However, RMON does require one probe per LAN segment (segments are separated by bridges or routers) and standalone RMON probes have traditionally been expensive.

Therefore, 3Com's approach has been to build an inexpensive RMON probe into the Transcend SmartAgent in each hub device. This allows RMON to be widely deployed around the network without costing more than traditional network management.

One other problem with standalone RMON probes is that they are passive, able to monitor and report but nothing more. Placing probe functionality inside the network device allows integration of RMON with normal device management to allow proactive management. For example, statistics can be related to individual hub ports and the hub can take autonomous actions such as disabling a port (temporarily or permanently) if errors on that port exceed a pre-defined threshold.

Also, since a probe needs to be able to see all traffic, a standalone probe has to be attached to a non-secure hub port. Implementing RMON in the hub means all hub ports can have security features enabled.

Integrating RMON into Transcend SmartAgents also allows other features to be incorporated to make RMON easier to use. Examples of this include:

- the AutoCalibrate feature, which records the peak value of a network statistic over time and in a single operation automatically sets a threshold at 120% of that peak value.
- the Remote Poller feature, which allows the hub to ping another device on the network and record the response time. An RMON Alarm can be associated with that response time so that when the response time from the server is poor because of an overloaded server or faulty cable the hub can inform the network administrator automatically.
- additional Actions-on-Event are also available when alarm thresholds are exceeded, to automatically disable ports, blip ports (switch off and then back on) or switch to a backup link.

The RMON capabilities of 3Com hubs can only be accessed through SNMP applications, not through the serial interface or Telnet. For more information about the details of managing 3Com devices using RMON, see the user documentation for Transcend Network Management Applications for Windows and UNIX.

The SuperStack II Hub 10 RMON Implementation

The following table summarizes the support in this product for the nine standard groups of RMON. The table also specifies the configuration of the various groups after system initialization.

Table E-1 RMON Group Configurations

Group	Initial Configuration	Effect of Power Cycle on Configuration
Ethernet Statistics	1 session monitoring the Ethernet repeater traffic.	configuration lost
Stats History	3 default sessions: a) 60 second interval, 120 historical samples stored. b) 30 second intervals, 120 historical samples stored. c) 30 minute intervals, 96 historical samples stored.	configuration lost
Host Table	1 session collecting host information.	configuration lost
Matrix Table	1 session collecting matrix information.	configuration lost
Host top 'N'	No default topN groups.	configuration lost
Alarm	Default alarms are configured at startup.	configuration restored
Event	Default events exist to describe our 'action-on-event' system. User can create new events.	configuration restored
Filter	Full packet filter is supported.	configuration lost
Capture	Full packet capture is supported on the Module.	configuration lost

After the default sessions are created, they have no special status. The user can delete or change these parameters as required.

Two default alarms are created initially. These are bandwidth used and errors /10000 packets. These can be deleted or changed as required.

RMON, in the SuperStack II implementation, is a very user configurable system. The user can create multiple monitoring facilities to run in parallel. Examples of these facilities may be:

- monitor all statistics,
- learn all the hosts,
- create a who-talks-to-whom matrix.

Because the SuperStack II Hub 10 stack supports only one Ethernet segment, there is one interface that can gather RMON information.

For those resources created by the RMON agent itself during startup, the owner string will be set to 'monitor'.

RMON monitoring requires considerable processing power. During extremely heavy traffic, the SuperStack II Hub 10 Management Module can become swamped and may not process data. Usually, this has a negligible effect. If you want to be sure to collect all data, we recommend you use the Advanced RMON Module with its faster processor and increased memory. Also you should use the Advanced RMON Module if you need memory-hungry statistics; for instance prolonged packet capture sessions.

The Management Information Base (MIB)

At the heart of all network management is the Management Information Base or MIB. It cannot be stressed too much how important it is to understand the nature of the MIB if you are to achieve the maximum potential offered by the management system.

The MIB is a formal structured set of data describing the way the network is functioning. The management software (the agent) accesses the set and abstracts the information it requires. The agent will also store data in the MIB.

The organization of the MIB is such that an SNMP network management package (for example, Transcend) without specific knowledge of a particular device can manage that device at an adequate level. This is known as Generic Network Management.

In simple terms, a MIB consists of a large number of objects which represent features of the equipment to be controlled and managed. An example of an object might be a port that can be enabled or disabled, or a counter that can be read.

Consider a counter object that records the number of frames transmitted onto the network. The MIB would contain the following entry:

```
a3ComEtherStatTxBytes OBJECT-TYPE
SYNTAX              Counter
ACCESS              read-only
STATUS              mandatory
DESCRIPTION         "This is a total count of all bytes placed on the
                    segment that originate from this station.
                    Neither the destination nor the type of
                    information is considered for this counter."
::= {a3ComEtherStatEntry 15}
```

In simple terms, this tells us:

1. The formal name of the counter is *3ComEtherStatTxBytes*. (3Com, Ethernet, Statistics, Transmit Bytes).
2. The counter is to be found in a table called *3ComEtherStat*.
3. The counter is the 15th column in the table.

It is not necessary to know and understand the MIB in order to manage a network. With most management facilities the MIB is transparent. But if you do have an understanding of how the various management features are derived, you will be in a better position to make full use of the information presented.

If you would like to have a copy of the MIB, contact 3Com using one of the means listed in Appendix B.

Counters

Counters are the MIB objects which hold and update the number of occurrences of a particular event through a port, module, repeater or on the network. The management facility reads the counters it needs for the output, processes the information and displays the result. The counter may be associated with a port, or a module, or a repeater, or even a chassis. It can be counting any recurring event: typical examples are traffic, collisions, and FCS errors.

When a port is disabled, some of the statistics counters associated with it may no longer be updated.

When using the counters, it is better to employ differences between values rather than spot values. By using values at fixed time intervals the rates of change of the counters can be derived. The time intervals can be as short or as long as you find convenient. These rates will be more meaningful than spot values and may be compared to provide more useful data.

There is a sound reason for using differences. The counters cannot be infinite. They will roll-over (return to zero) when they reach their limit. Thus a low value may or may not be truly representing the situation. A negative difference indicates that roll-over has occurred. You can be more sure of what has occurred by changing (either shortening or lengthening) the time interval and comparing the results.

Counters and RMON Alarms

The Module supports the RMON alarm. Alarms can be assigned by Transcend or any SNMP network manager to monitor any counter. Consult the manual of the application you use for details of how to set up the possible 1024 alarms.

Each alarm monitors its assigned counter, by calculating the differences over a preset time interval. It remembers the high and low tide marks and it can take actions when the value of the counter has crossed preset thresholds.

The diagram below shows the variation of a typical counter with time.

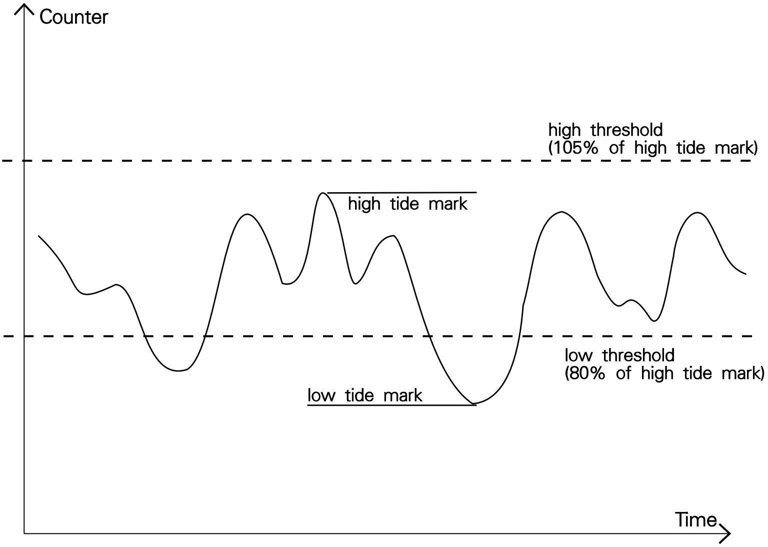


Figure E-1 Counter Values During Autosetting Of Thresholds

Alarm thresholds may be autocalibrated or set manually. Autocalibration is a means of calculating alarm thresholds specific to the activity of the counter being monitored. For autocalibration, the high threshold is set to 5% above the high tide mark. Also, the low threshold is set to 20% below the high tide mark (see diagram above).

Manually, you may choose any value for the thresholds using your network manager.

The tide marks are monitored continually during normal running to provide data for later calibration. This explains the high tide mark being above the threshold level in the diagram below.

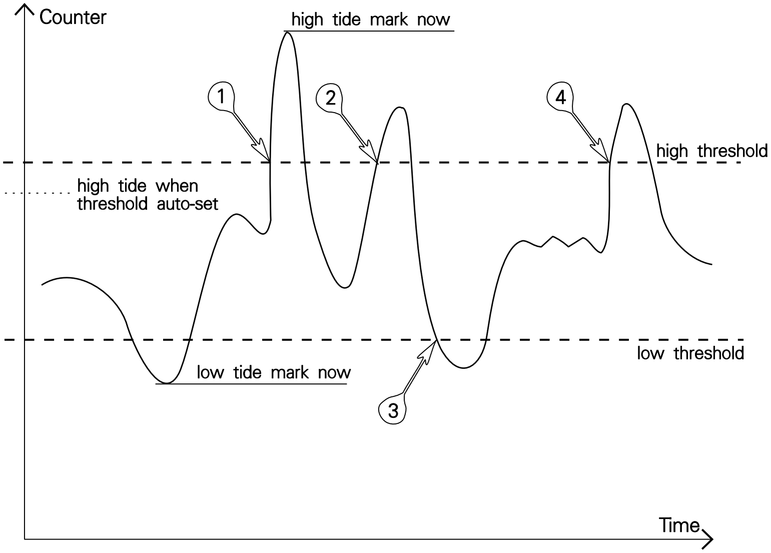


Figure E-2 Counter Values After Setting Thresholds

Alarms can be set up with two actions; one is associated with the high threshold and the other with the low threshold. Whether an action is taken depends on the circumstances surrounding each crossing of a threshold. The numbered paragraphs below describe the conditions applying at the points correspondingly numbered in the diagram.

1. The running value has exceeded the high threshold. If an action has been assigned to the high threshold, that action will be performed.
2. No action will be taken because the value has not fallen below the low threshold before rising above the high threshold. This gap between high and low thresholds is called Alarm Hysteresis.
3. The running value has fallen below the low threshold. If an action has been assigned to the low threshold, that action will be performed.
4. The running value had fallen below the low threshold before rising above the high threshold. If an action has been assigned to the high threshold, that action will be performed.

Table E-2 Alarm Actions

Action	High Threshold	Low Threshold
No action.		
Notify only.	Send Trap.	
Notify and blip port.	Send Trap. Turn port off. Turn port on after 5 seconds.	
Notify and disable port.	Send Trap. Turn port off.	
Notify and enable port.		Send Trap. Turn port on.
Blip port.	Turn port off. Turn port on after 5 seconds.	
Disable port.	Turn port off.	
Enable port.		Turn port on.
Notify and switch resilient port.	Send Trap. If port is the Main of a resilient pair then switch to standby.	
Notify and blip module.	Send Trap. Turn all ports on module off. Turn ports back to original state after 5 seconds.	
Notify and disable module.	Send trap. Turn all ports on module off.	
Notify and enable module.		Send Trap. Turn ports back to original state.
Blip module.		Turn all ports on module off. Turn ports back to original state after 5 seconds.
Disable module.	Turn all ports on module off.	
Re-enable module.		Turn ports back to original state.

Using Alarms

How to set up alarms is described in the manuals of your management application.

The alarm carries the ability to define actions to be taken when the alarm value rises above the high threshold, and/or falls below the low threshold.

Two system alarms with default values will be automatically set up for each port at initialization and whenever a new module is detected. The system alarms form part of the 1024 maximum. The system alarms are set up on the Smart Objects:

- Percentage Bandwidth Used
- Errors per 10,000 frames

The system alarms can be modified, but cannot be created or deleted by a user. The default values are given in the table below.

Table E-3 Smart Object Default Values

Parameter	**Traffic Level**	**Errors/10000 frames**
high threshold	15%	200
low threshold recovery	10%	100
samples per average	4	4
period	15 seconds	15 seconds

Once alarms have been set up on a module in a particular slot, they will be retained against that slot in any new configuration. This situation may be made clearer by the following examples.

> If a module is removed and replaced by a similar module, the alarms will be retained on the new module.
>
> If a module is swapped to another repeater backplane bus, the alarms will be retained on that module.

Here is an example of how you may benefit from the power of alarms.

Broadcast Storms are capable of using most of the available bandwidth of your network. If you set up an alarm on the Broadcast Frames Received counter of a port, with the 'Notify and Blip' action (see Table E-2 on page E-10), on the high threshold. If a broadcast storm occurs on that port and the counter crosses the high threshold, the port will disabled for 5 seconds, allowing the storm to subside and preventing the storm from reaching the rest of the network.

Audit Log

The Module keeps an audit log of all management user sessions, providing a record of changes to the configuration database (MIB). The log can be read only by a manager at the security (i.e. highest) access level using an SNMP network manager.

Each entry in the log is in the format:

Entry number timestamp user ID item ID (including qualifier) new value of item

There is a limit of 40 records on the number of changes stored. The oldest records are overwritten first.

F INDEX OF MANAGEMENT ACTIONS AND DATA

This index consists of an alphabetical listing of field names taken from the VT100 screens. It relates the field names to the page in the user guide where you can find a description of the use of the field and the title of the screen containing it. Also, it indicates the type of field.

Use the standard subject index which follows to look up general topics.

The “Key” column contains a code letter for the type of parameter presented. The meanings of these code letters is tabulated below. The “Page” column gives the page number in the current user guide where the use of the parameter is described. The “Screen” column gives the title of the screen where the parameter appears.

Code letter	Meaning
B	Button to next screen
C	Choose from toggle list
D	Direct action button
E	Enter text
R	Read-only data
S	Select from list

Parameter	Key	Page	Screen
Access Level	C	3-20	Create Users Screen
Active Port	C	3-28	Repeater Resilience
Active Port	C	3-39	Port Resilience
Active Power Supply	R	3-33	Unit Setup

Parameter	Key	Page	Screen
Alignment Errors	R	3-26	Repeater Statistics
Alignment Errors	R	3-31	Unit Statistics
Alignment Errors	R	3-35	Port Statistics
APPLY	D	3-39	Port Resilience
Area (of fault)	R	3-47	Fault Log
Autoconfig(uration)	C	3-15	Serial Port Setup Screen
Autopartitions	R	3-26	Repeater Statistics
Autopartitions	R	3-31	Unit Statistics
Autopartitions	R	3-35	Port Statistics
Bandwidth Used	R	3-26	Repeater Statistics
Bandwidth Used	R	3-31	Unit Statistics
Bandwidth Used	R	3-35	Port Statistics
Boot Software Version	R	3-45	Status Screen
Broadcast Frames	R	3-26	Repeater Statistics
Broadcast Frames	R	3-31	Unit Statistics
Broadcast Frames	R	3-35	Port Statistics
Char Size	R	3-15	Serial Port Setup Screen
CLEAR COUNTERS	D	3-26	Repeater Statistics
CLEAR COUNTERS	D	3-31	Unit Statistics
CLEAR COUNTERS	D	3-35	Port Statistics
Community String	C	3-21	Edit User Screen
Community String	E	3-20	Create Users Screen
Community String	E	3-13	Setup Traps Screen
Community-SNMP	C	3-18	Local Security Screen
Connection Type	C	3-15	Serial Port Setup Screen
CREATE USERS	B	3-17	User Access Level Menu
Data Link Protocol	R	3-10	Setup Menu
Data Rate Mismatches	R	3-26	Repeater Statistics
Data Rate Mismatches	R	3-31	Unit Statistics
Data Rate Mismatches	R	3-35	Port Statistics
DCD Control	C	3-15	Serial Port Setup Screen

Parameter	Key	Page	Screen
Default Router	E	3-10	Setup Screen
DELETE	D	3-39	Port Resilience
DELETE USERS	B	3-17	User Access Level Menu
DELETE USERS	D	3-21	Delete Users Screen
Device IP Address	E	3-10	Setup Screen
Device SubNet Mask	E	3-10	Setup Screen
DRS Control	C	3-15	Serial Port Setup Screen
EDIT USER	B	3-17	User Access Level Menu
Errors/10000 Packets	R	3-26	Repeater Statistics
Errors/10000 Packets	R	3-31	Unit Statistics
Errors/10000 Packets	R	3-35	Port Statistics
FAULT LOG	B	3-45	Status Menu
Fault Number	R	3-47	Fault Log
FCS Errors	R	3-26	Repeater Statistics
FCS Errors	R	3-31	Unit Statistics
FCS Errors	R	3-35	Port Statistics
Filename	E	3-50	Software Upgrade
Flow Control	C	3-15	Serial Port Setup Screen
Good Frames	R	3-26	Repeater Statistics
Good Frames	R	3-31	Unit Statistics
Good Frames	R	3-35	Port Statistics
Good Octets	R	3-26	Repeater Statistics
Good Octets	R	3-31	Unit Statistics
Good Octets	R	3-35	Port Statistics
Hardware Version	R	3-45	Status Screen
INITIALIZE	B	3-9	Main Menu
IP or IPX Address (for traps)	E	3-13	Setup Traps Screen
IPX Network	E	3-10	Setup Screen
Last Reset Type	R	3-45	Status Screen
Last Source Address	R	3-35	Port Statistics
Late Events	R	3-26	Repeater Statistics

Parameter	Key	Page	Screen
Password	E	3-21	Edit User Screen
POLL	D	3-44	Remote Poll
Port ID	E	3-22	Repeater Management
Port ID	R	3-35	Port Statistics
Port ID	R	3-36	Port Setup
Port State	C	3-36	Port Setup
Power Supply Status	R	3-33	Unit Setup
REMOTE POLL	B	3-9	Main Menu
Remote Telnet (Security)	C	3-18	Local Security Screen
Repeater Health	R	3-27	Repeater Setup
REPEATER MANAGEMENT	B	3-9	Main Menu
RESET	B	3-9	Main Menu
Reset Count	R	3-47	Fault Log
RESILIENCE	B	3-22	Repeater Management
Round Trip Time	R	3-44	Remote Poll
Runt Frames	R	3-26	Repeater Statistics
Runt Frames	R	3-31	Unit Statistics
Runt Frames	R	3-35	Port Statistics
SECURITY	B	3-9	Main Menu
Security	C	3-36	Port Setup
SELF TEST	B	3-9	Main Menu
Serial Port (Security)	C	3-18	Local Security Screen
SERIAL PORT	B	3-10	Setup Screen
Server IP Address	E	3-50	Software Upgrade
SETUP	B	3-9	Main Menu
SETUP	B	3-22	Repeater Management
SETUP TRAPS	B	3-10	Setup Screen
Short Events	R	3-26	Repeater Statistics
Short Events	R	3-31	Unit Statistics
Short Events	R	3-35	Port Statistics
SLIP Address	E	3-10	Setup Screen

Parameter	Key	Page	Screen
SLIP SubNet Mask	E	3-10	Setup Screen
Source Address Changes	R	3-35	Port Statistics
Speed (serial line)	C	3-15	Serial Port Setup Screen
Standby Links Available	R	3-39	Port Resilience
Standby Port	R	3-28	Repeater Resilience
Standby Port ID	C	3-39	Port Resilience
Standby Unit	R	3-28	Repeater Resilience
Standby Unit ID	C	3-39	Port Resilience
STATISTICS	B	3-22	Repeater Management
STATUS	B	3-9	Main Menu
Status	C	3-10	Setup Screen
Stop Bit	R	3-15	Serial Port Setup Screen
SOFTWARE UPGRADE	B	3-9	Main Menu
System Up Time	R	3-45	Status Screen
Target Address	E	3-44	Remote Poll
Throttle	E	3-13	Setup Traps Screen
Time (since reset)	R	3-47	Fault Log
Too Long Frames	R	3-26	Repeater Statistics
Too Long Frames	R	3-31	Unit Statistics
Too Long Frames	R	3-35	Port Statistics
Total Collisions	R	3-31	Unit Statistics
Total Collisions	R	3-35	Port Statistics
Total Errors	R	3-26	Repeater Statistics
Total Errors	R	3-31	Unit Statistics
Total Errors	R	3-35	Port Statistics
Total Ports Partitioned	R	3-27	Repeater Setup
Transceiver Module	R	3-33	Unit Setup
Transmit Collisions	R	3-26	Repeater Statistics
Unauthorized Device Action	C	3-36	Port Setup
Unicast Frames	R	3-26	Repeater Statistics
Unicast Frames	R	3-31	Unit Statistics

Parameter	Key	Page	Screen
Unicast Frames	R	3-35	Port Statistics
Unit Boot State	R	3-33	Unit Setup
Unit Capacity	R	3-27	Repeater Setup
Unit Hardware Revision	R	3-33	Unit Setup
Unit ID	E	3-22	Repeater Management
Unit ID	R	3-31	Unit Statistics
Unit ID	R	3-35	Port Statistics
Unit ID	R	3-33	Unit Setup
Unit ID	R	3-36	Port Setup
Unit Port Capacity	R	3-33	Unit Setup
Units Available	R	3-27	Repeater Setup
Unit Type	R	3-33	Unit Setup
Unit Type	R	3-31	Unit Statistics
Upgradeable Software Version	R	3-45	Status Screen
User List	S	3-21	Delete User Screen
User Name	E	3-7	Logon Screen
User Name	E	3-10	Auto Logout Screen
User Name	E	3-20	Create User Screen
User Name	E	3-21	Edit User Screen
Very Long Events	R	3-26	Repeater Statistics
Very Long Events	R	3-31	Unit Statistics
Very Long Events	R	3-35	Port Statistics

INDEX

ELECTRO-MAGNETIC COMPATABILITY STATEMENT

FCC Statement

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

CSA Statement

This Class A digital apparatus meets all requirements of the Canadian interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences

LIMITED WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	**One year**
Network adapters	**Lifetime**
Ethernet stackable hubs and Unmanaged Ethernet fixed port repeaters	**Lifetime*** **(One year if not registered)**
***Power supply and fans in these stackable hubs and unmanaged repeaters**	**One Year**
Other hardware products	**One Year**
Spare parts and spares kits	**90 days**

If a product does not operate as warranted during the applicable the warranty period, 3Com shall, at its expense, correct any such defect by repairing the defective product or part or, at its option, by delivering to Customer an equivalent product or part to replace the defective item. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com pursuant to any warranty.

SOFTWARE: 3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the magnetic media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation hereunder shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party's product.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt by 3Com.

WARRANTIES EXCLUSIVE: IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

Limitation of Liability. IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) SHALL 3COM BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Some states do not allow the exclusion of implied warranties or the limitation of incidental or consequential damages for consumer products, so the above limitations and exclusions may not apply to you. This warranty gives you specific legal rights which may vary from state to state.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95052-8145
(408) 764-5000