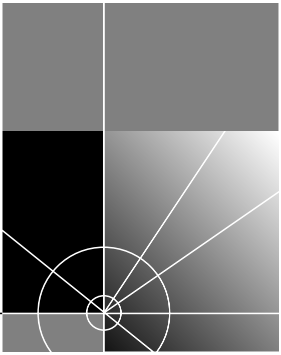
SuperStack® II Dual Speed Hub 500 Management Module User Guide

Software Version: 2.14

http://www.3com.com/

Part No. DUA1668-5AAA04
Published November 2000



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

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

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, 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.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

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

3Com, the 3Com logo, Dynamic*Access*, Net Age, SmartAgent, SuperStack, and Transcend are registered trademarks of 3Com Corporation. ATMLink, AutoLink, CoreBuilder, FDDILink, NetProbe, and PACE are trademarks of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is 3Com’s policy to be environmentally friendly in all its operations. This manual is printed on paper that comes from sustainable, managed European forests. The production process for making the pulp has a reduced AOX level (adsorbable organic halogen) resulting in elemental chlorine free paper.

The paper is fully bio-degradable and recyclable.

CONTENTS

IMPORTANT SAFETY INFORMATION

L'INFORMATION DE SÉCURITÉ IMPORTANTE

WICHTIGE SICHERHEITSHINWEISE

ABOUT THIS GUIDE

1 OVERVIEW AND INSTALLATION OF THE MANAGEMENT MODULE

2 MANAGING THE DUAL SPEED HUB 500

3 USING THE COMMAND LINE INTERFACE

IMPORTANT SAFETY INFORMATION

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

Please read the following safety information thoroughly before installing the Dual Speed Hub Management Module.

Installation and removal of the module must be carried out by qualified personnel only. Before installing the module into a unit, you must first disconnect the unit from the mains power supply. For full safety instructions, refer to the user guide that accompanies the unit.

U.K. Users Only
The Dual Speed Hub 500 Management Module is covered by Oftel General Approval, NS/G/12345/J/100003, for indirect connection to a public telecommunications system. This can be achieved using the console port on the Dual Speed Hub 500 and an approved modem.

L'INFORMATION DE SÉCURITÉ IMPORTANTE

AVERTISSEMENT: *Les avertissements contiennent les directions que vous devez suivre pour votre sécurité personnelle. Suivez toutes les directives avec soin.*

Veuillez lire à fond l'information de la sécurité suivante avant d'installer le Dual Speed Hub Management Module.

Confiez l'installation et la dépose de ce module à un personnel qualifié. Avant d'installer ce module dans un groupe, vous devez au préalable débrancher ce groupe de l'alimentation secteur. Pour prendre connaissance des consignes complètes de sécurité, consultez le guide utilisateur qui accompagne ce groupe.

WICHTIGE SICHERHEITSHINWEISE

***WARNHINWEIS:** Warnungen enthalten Anweisungen, die zur eigenen Sicherheit unbedingt zu beachten sind. Bitte befolgen Sie alle Anweisungen sorgfältig und genau.*

Bitte unbedingt vor dem Einbauen des Dual Speed Hub Management Module Einheit die folgenden Sicherheitsanweisungen durchlesen.

Die Installation und der Ausbau des Moduls darf nur durch Fachpersonal erfolgen. Vor dem Installieren des Moduls in einem Gerät muß zuerst der Netzstecker des Geräts abgezogen werden. Vollständige Sicherheitsanweisungen sind dem Benutzerhandbuch des Geräts zu entnehmen.

ABOUT THIS GUIDE

This guide describes how to install the SuperStack® II Dual Speed Hub Management Module, and how to use the management systems it provides to manage the Dual Speed Hub 500.

This guide is intended for users who have networking experience. If you have not managed a networking product before, we recommend that you read through this guide before using the hub, so that you can gain knowledge of the features and how you can use them.

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

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

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

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
ℹ	Information note	Information that describes important features or instructions
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Commands`	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To exit, enter the following command: **`logout`** When using the command line interface, only the first few letters of each command need to be typed (the letters that make the command unique from the other commands). For example, you can enter **`l`** to exit the command line interface, instead of typing the whole command.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Related Documentation

The following documents accompany this user guide:

- *Quick Reference Guide*

  This contains some useful information from this guide which you may need to refer to regularly.

The following documentation accompanies the Dual Speed Hub 500:

- *Dual Speed Hub 500 User Guide*

  This contains information on how to install and use the Dual Speed Hub 500.

Product Registration

You can now register your SuperStack II Dual Speed Hub 500 Management Module on the 3Com Web site to receive up-to-date information on your product:

`http://support.3com.com/registration/frontpg.pl`

Year 2000 Compliance

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

`http://www.3com.com/products/yr2000.html`

Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commencing:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- Dual Speed Hub 500 Management Module User Guide
- Part Number DUA1668-5AAA03
- Page 25

1 OVERVIEW AND INSTALLATION OF THE MANAGEMENT MODULE

This chapter contains the following topics:

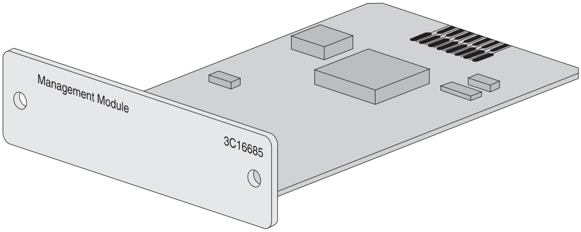
- An introduction to the management module and the products it can be used with
- How the management module can be used
- Installing and removing the management module

Introduction

The SuperStack® II Dual Speed Hub Management Module, as shown in Figure 1, is an easy to use management module that provides SNMP and RMON support for the SuperStack II Dual Speed Hub 500 range of units. It also enables a number of automatic features that enhance the capabilities of the Dual Speed Hub 500, including:

- Security
- Resilient links

Figure 1 The SuperStack II Dual Speed Hub Management Module



The management module can be used with the web interface or command line interface (provided free by the management module), or with a Transcend® network management application. For more information about these management methods, refer to "How You Can Manage the Dual Speed Hub 500" on page 26.

Smart Auto-sensing Feature

Smart auto-sensing only works if it is enabled (it is enabled for the stack by default) and the device to which the port is connected supports 10/100 auto-negotiation.

When a 100Mbps connection is made to one of the ports on the Dual Speed Hub 500, the Smart auto-sensing feature checks the quality of the connection. If the connection is unsuitable (probably due to low quality cabling or too many patch panel connections), Smart auto-sensing will automatically downgrade the port to operate at 10Mbps. The LED for that port (on the front of the unit) is changed to reflect the new speed, and a warning trap is sent to the management station (if traps have been configured).

If you subsequently repair a faulty link that has been downgraded by Smart auto-sensing, the feature will automatically recheck the connection as soon as the link is made.

When the management module is used with Dual Speed Hub 500 units running management agent software version 1.11 or later, the Smart auto-sensing feature can be managed for the stack.

You may disable the Smart auto-sensing feature for the entire stack. For information on doing this using the web interface, refer to "Smart Auto-sensing" on page 98. Alternatively, you can fix a particular port to either 10Mbps or 100Mbps while allowing other ports to engage in Smart auto-sensing, refer to "Port Setup" on page 86.

Management of the Dual Speed Hub 500

The management module can be fitted into either of the two transceiver module slots in the Dual Speed Hub 500, and provides management for the whole stack.

Currently the management module can be used with these units:

- 3C16610 — SuperStack II Dual Speed Hub 500 12-port
- 3C16611 — SuperStack II Dual Speed Hub 500 24-port

Contact your supplier for information about any other units that the management module may be used with. For information on how to use the Dual Speed Hub 500, refer to the documentation that accompanies the hub.

Management of the Distance Extender Modules

The Dual Speed Hub 500 can be fitted with these modules:

- 3C16683 — 100BASE-TX Distance Extender Module
- 3C16684 — 100BASE-FX Distance Extender Module

The slide-in modules for the Dual Speed Hub 500 are not hot-swappable. Swapping modules while the unit is powered on will result in the module port being disabled until the unit is powered off and on again. Please follow the instructions for the correct procedures given in "Installing and Removing the Management Module" on page 19.

The Half/Full Duplex selector on the 100BASE-FX Distance Extender Module is not intended for hot-selection. The correct procedure for changing the Duplex mode is to power off the unit, set the selector and power on the unit.

The management module allows you to manage the operation of these modules in the stack. For an overview of the management you can perform, refer to "Management of the Distance Extender Modules" on page 25.

Management of a Different Hub or Stack

A different hub or stack can be connected to the Dual Speed Hub 500 stack using a Cascade Converter Kit. A Dual Speed Hub 500 – Hub 10 Cascade Converter Kit (part number 3C16686) is available allowing you to connect a managed Hub 10 stack directly to the Dual Speed Hub 500 stack. For information on installing and using the Cascade Converter Kit, refer to the user guide that accompanies it.

The management module allows you to access the management screens of an attached hub or stack (such as a Hub 10 stack) while managing the Dual Speed Hub 500. For information on doing this using the web interface, refer to "Accessing a Different Hub or Stack" on page 101.

How the Management Module Can Be Used

The management module can be fitted into either of the transceiver module slots in the Dual Speed Hub 500; refer to "Installing the Management Module" on page 20 for information on how to do this.

When multiple Dual Speed Hub 500 units are connected together with cascade cables, they form a single hub (called a *stack*). The management module can be fitted into any one of the units and provides management for the whole stack.

Management Resilience

Protection Against Unit Failure

The cascade cables that carry the network and management communication between the units in the stack, have resilience built into them which protects the communication channel should a unit fail. You can further this resilience by using Hot Swap Cascade Units, which allow you to remove and replace units in the stack, without affecting the other units in the stack.

For more information about Hot Swap Cascade Units, contact your supplier.

Protection Against Losing Management

If the stack splits in two (if one of the cascade cables becomes disconnected), one half of the stack will lose connection to the management module if there is just one management module in the stack. You can protect against this by having multiple management modules in the same stack (for example one in the top unit and one in the bottom unit). Then, if the stack does split, both halves can be managed because they both have access to a management module.

Installing and Removing the Management Module

Before You Start

WARNING: *Ensure you have read the Important Safety Information section carefully before you start.*

AVERTISSEMENT: *Assurer que vous avez lu soigneusement la section de L'information de Sécurité Importante avant que vous commenciez.*

WARNHINWEIS: *Versichern Sie sich, daß Sie den Abschnitt mit den wichtigen Sicherheitshinweisen gelesen haben, bevor Sie das Gerät benutzen.*

Handling the Management Module

CAUTION: *The management module can be damaged easily by electrostatic discharge.*

To prevent damage, please observe the following:

- Do not remove the management module from its packaging until you are ready to install it into the hub.
- Do not touch any of the pins, connections or components on the management module.
- Handle the management module only by its edges and front panel.
- Always wear an anti-static wristband connected to a suitable earth point.
- Always store or transport the management module in appropriate anti-static packaging when not in use.

Installing the Management Module

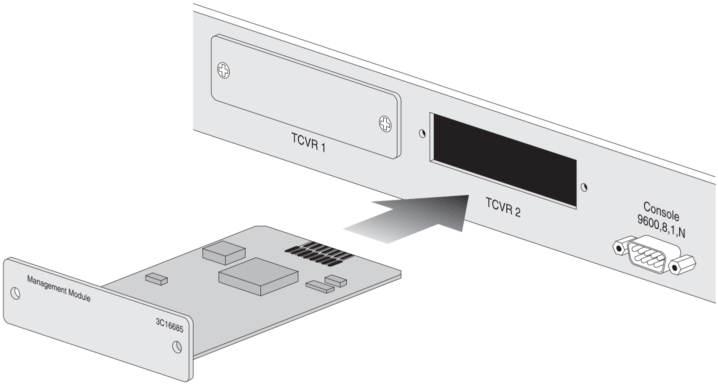
Before you install the management module, please ensure that any equipment to be attached to the Dual Speed Hub 500 has the latest version of its driver software installed, especially any network interface card.

The slide-in modules for the Dual Speed Hub 500 are not hot-swappable. Swapping modules while the unit is powered on will result in the module port being disabled until the unit is powered off and on again. Please follow the instructions for the correct procedure for inserting and removing the modules given below.

To install the management module into the Dual Speed Hub 500:

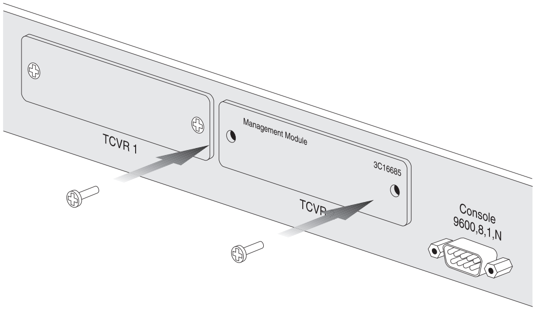
1. Ensure that the hub is disconnected from the power supply, and that you are wearing an anti-static wristband connected to a suitable earth point.
2. Place the hub on a flat surface. Using a suitable screwdriver, remove the blanking plate that covers the transceiver module slot (on the rear of the hub) that you are going to insert the management module into (you can use either slot). Do not remove any other screws from the rear of the hub. Refer to the user guide supplied with the hub if uncertain of the position of the blanking plate.
3. Keep the blanking plate in a safe place. If you remove the management module at any time, you must replace the blanking plate to prevent dust and debris entering the hub and to aid the circulation of cooling air.
4. Hold the management module so that the text on the front panel is upright, and slide it into the hub, as shown in Figure 2, ensuring the edge connector is fully engaged. The front panel of the management module should lie flush against the rear panel of the hub.

Figure 2 Inserting the Management Module (either slot can be used)



5 Fix the front panel of the management module to the hub using the two screws from the blanking plate, as shown in Figure 3.

Figure 3 Fixing the Management Module in Place



Removing the Management Module

To remove the management module from the Dual Speed Hub 500:

1 Ensure that the hub is disconnected from the power supply, and that you are wearing an anti-static wristband connected to a suitable earth point.

2 Place the hub on a flat surface. Using a suitable screwdriver, remove the screws that hold the management module in place. Do not remove any other screws from the rear of the hub.

3 Remove the management module and place it in the packaging that it was supplied in (or other appropriate anti-static packaging).

4 Replace the blanking plate over the empty transceiver module slot in the rear of the hub, and use the two screws to fix the blanking plate in place.

For information on how the hub's configuration is affected by the removal of the management module, refer to "Removing Management From the Hub" on page 25.

Powering On the Hub or Stack

When you have fitted the management module correctly, you can power on the hub. If the hub is connected to other Dual Speed Hub 500 units with cascade cables, those units become managed units within 20 seconds.

For information on making a management connection to the hub or stack, refer to "Methods of Management" on page 28.

In rare circumstances, repeatedly powering units off and on in a stack may cause an interruption to the management of the stack. To avoid this, it is recommended that the bottom unit in the stack is powered on first, followed by the unit above it, and so on.

Upgrading the Smart Agent Version

Supplied with every management module you will find the latest management agent software. You should check the version on your Dual Speed Hub 500 by either:

- Entering **`system display`** on the Command Line Interface (CLI);

or

- Accessing the Unit Status page through the Web Interface.

If the version number is less than the version supplied with your management module, upgrade the agent following the instructions in "Upgrading the Management Software" on page 69 (CLI) or "Software Upgrade" on page 99 (Web interface).

2 MANAGING THE DUAL SPEED HUB 500

This chapter contains the following topics:

- An overview of the management provided by the management module
- What you can use to manage the hub or stack
- How you can make a management connection to the hub or stack

A stack of Dual Speed Hub 500 units is treated as a single manageable entity, and the management is distributed. This guide uses the word ‘**stack**’ to refer to a stack of one or more units, and ‘**management station**’ to refer to the piece of equipment you are using to manage the stack (for example a computer).

For an overview of the management tasks you can perform, refer to “Management Features” on page 24.

Management Features

With management, you can change and view the way the hub or stack operates.

Management of the Dual Speed Hub 500

Using the management interfaces that are provided by the management module (the command line interface and web interface), you can:

- Display a graphical representation of the stack and quickly view the status of each hub and its ports.
- Display general information for the hub or stack.
- Enable and disable ports.
- Configure Smart auto-sensing for the stack.
- Configure security for the ports, including specifying what equipment is allowed to communicate through the ports on the hub.
- Reset the IP information on the hub or the stack.
- Set up resilience; specify a backup connection that takes over should a main connection fail.
- View statistics.
- Configure the console port for connection to a modem.
- Configure security for the hub or stack; change the passwords for the management user levels.
- Upgrade the management software in the stack with any future management agent software upgrade.
- Restart the hub or stack to refresh its statistics and use any new configurations.
- Initialize the hub or stack to return it to its factory settings (any IP information that has been configured is retained).
- Configure the stack to send messages (called *traps*) to an SNMP network management application if certain conditions arise.

For an overview of the interfaces that are provided by the management module, refer to "How You Can Manage the Dual Speed Hub 500" on page 26.

3Com's Transcend® Enterprise Manager enables you to perform all of the tasks that the command line interface and web interface can. It also allows you to perform remote monitoring using RMON.

For more information about Transcend Enterprise Manager and other 3Com SNMP network management applications, refer to "SNMP Network Management" on page 27. For more information about RMON, refer to "RMON" on page 27.

Management of the Distance Extender Modules

Using the management interfaces that are provided by the management module, you can:

- Enable and disable the Distance Extender Module port.
- View traffic statistics, the link status and the port state.

Management of a Different Hub or Stack

If you have connected a different unit or stack to the Dual Speed Hub 500 stack with a Cascade Converter Kit, you can use the web interface that is provided by the management module to access the attached stack's management screens. For information on doing this, refer to "Accessing a Different Hub or Stack" on page 101. You can use the Dual Speed Hub 500 – Hub 10 Cascade Converter Kit to connect a Hub 10 stack to the Dual Speed Hub 500 stack.

Removing Management From the Hub

If the management module is removed from the hub (or the hub is separated from a unit with a module in it), there is a 3 minute period during which the hub remains managed (this is so that it is not affected by any quick disconnections between the units in the stack). If the hub does not have access to a management module after that period, the hub can no longer be managed but retains its configuration so that it can continue to operate as configured.

Without a management module, the hub cannot:

- Respond to any type of management communication
- Perform resilient links
- Generate SNMP traps
- Perform RMON

How You Can Manage the Dual Speed Hub 500

The management module includes two complete management interfaces for the Dual Speed Hub 500, that you can access locally (through the console port on the Dual Speed Hub 500) or remotely (over the network):

- **Command line interface** — can be used to set up network address information for the hub or stack.
- **Web interface** — provides easy 'point and click' graphical management of the hub or stack from any suitable Web browser.

Command Line Interface

The command line interface is a simple text-based user interface which allows you to configure some of the network information for the hub or stack. The command line interface provides a subset of the web interface's functionality but is intended as a quick setup tool, to get your hub ready for management over the network. You can use a terminal or terminal emulator to access the command line interface using a direct connection or across the network using Telnet (with IP configured).

For information on making a management connection to the command line interface, refer to "Command Line Interface" on page 31.

Web Interface

The web interface provides easy management of the hub or stack. It behaves in a similar way to a Web site on the World Wide Web, and you access it using a Web browser. The web interface is protected by a password panel, which prevents unauthorized access. You use the different pages of the web interface to change the network information in you hub or stack, and perform different management tasks.

For information on making a management connection to the web interface, refer to "Web Interface" on page 35.

SNMP Network Management

As your network grows, you may need a more powerful SNMP network management application that can control all of your managed units. Whether your network is large or small, its ongoing performance, growth and security are only as good as its management system.

3Com produces a range of powerful graphical SNMP network management applications (for example Transcend Enterprise Manager for Windows) that give you total control over your entire 3Com network from a single management station.

Using intelligent 3Com software distributed throughout the network (TranscendWare®), 3Com's management applications support all of today's platforms and manage a wide variety of 3Com products.

For further information about which Transcend management application can benefit your growing network, call your local sales office; refer to the Dual Speed Hub 500 User Guide for contacts.

Upgrading Your Transcend Management Application

If you currently use a Transcend management application to control your network, you must have these software versions (or later) for it to support the Dual Speed Hub 500:

- UNIX:
  - Transcend Enterprise Manager — Version 4.2.2
- Windows:
  - Transcend Enterprise Manager 97 for NT and software patch P0078
  - Transcend Enterprise Manager — Version 6.1 and software patch P0078
  - Transcend Workgroup Manager — Version 6.1 and software patch P0078

The documentation that accompanies your Transcend management application has information on obtaining and upgrading to a higher version.

RMON

The management module provides the Dual Speed hub 500 with *RMON* (Remote Monitoring) capabilities that can be used by network administrators to improve the efficiency of the network and reduce the load on the network.

You can only use the RMON features of the hub if you have an RMON management application, such as the RMON application supplied with 3Com's Transcend Enterprise Manager, or using a MIB browser.

RMON and the RMON capabilities of the Dual Speed Hub 500 are described in Appendix C, "RMON".

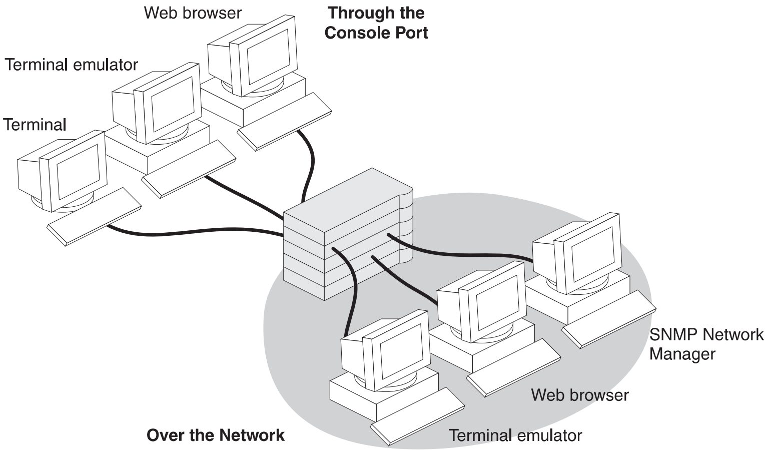
Methods of Management

There are many ways you can connect your management station to the stack, as shown in Figure 4. You can manage the stack:

- Through the console port (known as *out-of-band* management):
  - Using a Web browser
  - Using a terminal emulator
  - Using a terminal
- Over the network (known as *in-band* management):
  - Using a Web browser
  - Using a terminal emulator (over Telnet)
  - Using an SNMP network management application

If you are going to manage the stack over the network, the quickest way to set it up with the necessary network information is to connect to the console port on one of the units and use the command line interface.

Figure 4 Different Management Connections to the Stack



Requirements for Managing Over the Network

When managing your stack over the network, you must remember that (regardless of your method of management):

- The stack must be correctly configured with IP information. You must make a direct management connection through the console port to do this (or use a BOOTP server).

IP addresses are unique, no two units must have the same IP address. If you have no previous knowledge of IP, refer to “IP Addresses” *on* page 30.

If you have a BOOTP server, it can automatically assign your network equipment, including the Dual Speed Hub 500 units, with IP information so that it can be communicated with and managed over the network. Refer to the documentation that accompanies your BOOTP server for more information.

- Any IP information configured for a unit in the stack can be used to access the whole stack.
- IP must be correctly set up for your management station.
- You can manage the stack over the network, through any of the ports on the units. However, for the communication to work over

the network, the port through which your communication reaches the stack must not be disabled by management.

IP Addresses

If you are uncertain about what IP addresses to assign your equipment, contact your network administrator.

To operate correctly, each device on your network (for example a hub or management station) must have a unique IP address (if one is configured). IP addresses have the format *n.n.n.n* where *n* is a decimal number between 0 and 255. An example IP address is '192.168.100.8'.

The IP address can be split into two parts:

- The first part ('192.168' in the example) identifies the network on which the device resides.
- The second part ('100.8' in the example) identifies the device within the network.

If your network is internal to your organization only, you may use an arbitrary IP address. We suggest you use addresses in the series 192.168.100.*X* (where *X* is a number between 1 and 254) with a subnet mask 255.255.255.0. Use the default SLIP address of 192.168.101.1 with a subnet mask of 255.255.255.0.

These suggested IP addresses are part of a group of IP addresses that have been set aside specially for use "in house" only.

CAUTION: *If your network has a connection to the external IP network, you must apply for a registered IP address. This system ensures that every IP address used is unique; if you do not have a registered IP address, you may be using an identical address to someone else and your network will not operate correctly.*

Obtaining a Registered IP Address

InterNIC Registration Services is the organization responsible for supplying registered IP addresses. The following contact information is correct at time of publication:

World Wide Web site: **`http://www.internic.net`**

Command Line Interface

The command line interface allows you to configure a limited set of parameters for the unit. You can access the command line interface:

- Through the console port
- Over the network

This section has information on accessing the command line interface. For more information on using it, refer to Chapter 3"Managing the Dual Speed Hub 500".

Through the Console Port

Table 3 shows the settings for the hub's console port.

Table 3 Console Port Settings

Data bits (character size)	8
Stop bit	1
Parity	None

You can access the console port through a direct local connection, or you can set up a remote connection using a modem.

The terminal or management station (with the terminal emulator) connected to the console port must use the same settings as the unit. By default, the unit has auto-configuration enabled which changes the hub's console port settings to match those of the connected equipment and automatically detects the baud rate (line speed). The unit can auto-detect baud rates of 1200, 2400, 4800, 9600 and 19,200.

You need to use a null modem cable for connecting your terminal or management station directly to the console port. This should be available from your supplier. There are a variety of null modem cables that you can use. For an example of one of these, refer to "Examples of Null Modem Cables You Can Use" on page 113.

If you are using a modem in your setup, you need to use a modem cable. For an example of one of these, refer to "Modem Cable" on page 114. For information on setting up and connecting the modem, refer to the documentation that accompanies the modem.

To connect your equipment:

1 Connect the serial port on your terminal or management station to the console port on the unit, using a null modem cable.

2 Ensure that the terminal or management station’s serial port settings match those of the console port on the unit.

Using a Terminal Emulator

If you do not have a terminal, you can use a terminal emulator to access the command line interface. Microsoft Windows comes with a suitable terminal emulator:

- Windows 95 and Windows NT (version 4 or later) have a program called ‘HyperTerminal’.
- Other versions of Windows have a program called ‘Terminal’.

For other types of management stations and operating systems, refer to the documentation that accompanies your application for information on how to use it.

HyperTerminal

HyperTerminal can usually be found from the Windows *Start* menu, in *Programs*, *Accessories*. To start a HyperTerminal session (after connecting to the unit’s console port):

1 Double-click on the ‘Hypertrm.exe’ icon to start the application. The Connection Description dialog box appears.

2 Type a name for the session in the *Name* field and click *OK*. The Phone Number dialog box appears.

3 Select the serial port (for the management station) that you are using to connect to the unit, in the *Connect using* field.

The COM Properties dialog box appears.

4 Configure the fields as follows and click *OK*:

- **Bits per second** — any setting no higher than 19,200
- **Data bits** — 8
- **Parity** — None
- **Stop bits** — 1
- **Flow control** — None

5 Click in the main HyperTerminal window and press Return twice to start the communication.

Terminal

Terminal can usually be found from the Main window, in the *Accessories* program group. To start a Terminal session (after connecting to the unit's console port):

1 Double-click on the 'Terminal' icon to start the application.

2 If the Default Serial Port dialog box appears, select the serial port (for the management station) that you are using to connect to the unit and click *OK*.

3 From the *Settings* menu in the main Terminal window, select *Terminal Emulation*. The Terminal Emulation dialog box appears.

4 Select 'DEC VT-100 (ANSI)' and click *OK*.

5 From the *Settings* menu, select *Communications*. The Communications dialog box appears.

6 Configure the fields as follows and click *OK*:

- **Baud Rate** — any setting no higher than 19,200
- **Data Bits** — 8
- **Stop Bits** — 1
- **Parity** — None
- **Flow Control** — None

7 Click in the main Terminal window and press Return twice to start the communication.

Over the Network

You can access the CLI over a TCP/IP network using Telnet. To run Telnet, you need a suitable terminal or management station running a terminal emulator.

You can have multiple command line interface management sessions at the same time. If a connection is lost inadvertently, the connection is closed by the unit after about 30 minutes of inactivity.

Telnet

Microsoft Windows 95 comes with a suitable program called 'Telnet'. To open a Telnet session, you must specify the IP address of the unit you want to manage. For other types of management stations and operating systems, refer to the documentation that accompanies your Telnet terminal emulator for information on how to do this.

The Telnet application ('Telnet.exe') can usually be found in the *Windows* directory on your PC. To start a Telnet session:

1. Run the 'Telnet.exe' application. The Telnet application's window appears.
2. From the *Connect* menu, select *Remote System*. The Connect dialog box appears.
3. Type the IP address of the unit in the *Host name* field, select 'telnet' for the *Port* field, and select 'vt-100' for the *TermType* field.
4. Click *Connect.*

Web Interface

You can manage the stack using the management module's web interface. You can access the web interface:

- Through the console port
- Over the network

This section has information on accessing the web interface. For more information on using the web interface, refer to Chapter 4"Managing the Dual Speed Hub 500"..

Through the Console Port

You can access the web interface through the console port of a unit in the stack, using a management station running *SLIP* (Serial Line Interface Protocol).

If your management station is running Windows 95, you must use a SLIP driver that sets up SLIP access for web interface management. A suitable SLIP driver (the 3Com serial web utility) is supplied on the CD-ROM that accompanies the management module. To install and use the 3Com serial web utility, refer to Appendix B.

You need to use a null modem cable for connecting your management station directly to the console port. This should be available from your supplier. There are a variety of null modem cables that you can use. For an example of one of these, refer to "Examples of Null Modem Cables You Can Use" on page 113.

Over the Network

You must have IP software correctly installed on your management station and a connection to the local network, to be able to manage over a TCP/IP network. An easy way to check this is that if you have access to the Internet and can download Web pages from it, your management station has already got correctly installed IP software.

Which Web Browsers are Supported?

To access the web interface correctly, your Web browser must support:

- JAVA®
- Frames
- HTML 3.2

Suitable Web browsers are:

- Netscape Navigator Version 3.0 or later
- Microsoft Internet Explorer Version 3.0 or later

For information on using your Web browser, or finding out what it supports, refer to the documentation that accompanies it or visit the Web site of the company that produces your Web browser.

The web interface displays on screens that have 16 colors and a resolution as low as 640 x 480 pixels. However, the ideal screen setup should have at least 256 colors and a resolution of 800 x 600 pixels.

Configuring Your Browser

Before you use your Web browser to access the web interface, you must make one small configuration change to it, so that it always downloads the latest version of a page.

To do this for Netscape Navigator:

1. Start Netscape Navigator.
2. From the *Options* menu, select *Network Preferences*. The preferences dialog box appears.
3. Select the *Cache* tab.
4. In the Cache property sheet, check the 'Every Time' checkbox.
5. Click *OK*.

To do this for Microsoft Internet Explorer:

1. Start Microsoft Internet Explorer.
2. From the *View* menu, select *Options*. The Options dialog box appears.
3. Select the *Advanced* tab, and in the Advanced property sheet click *Settings*.
4. Check the 'Every visit to the page' checkbox.
5. Click *OK*.

3 USING THE COMMAND LINE INTERFACE

This chapter describes how to use the command line interface. The command line interface is a quick and simple interface which allows you to enter various IP address settings, reset the stack and initialize the stack. The web interface can perform most of the tasks that the command line interface can do.

You would normally use the command line interface if you have many units that you want to set up quickly with IP address information, for eventual management using an SNMP network management application. Simple help is provided with each command in the command line interface.

Ensure that your terminal or management station (which has the terminal emulator) has been appropriately set up for your particular management method and that any necessary connections have been made. Refer to "Command Line Interface" on page 31.

If you have any problems using the command line interface, refer to "Solving Problems With the Command Line Interface" on page 106.

Accessing the Command Line Interface

By default, the Dual Speed Hub 500 automatically configures the baud rate of its console port to operate with the connected management station or terminal, provided the parity, stop bits and character size are identical to the connected management station or terminal. You may need to perform the wake-up procedure to initiate the communication. To do this, press Return several times at the management station or terminal.

The login sequence for the command line interface begins as soon as the hub detects a connection to its console port, or as soon as a Telnet session is started.

Initial Access

The `Login:` prompt is displayed.

As the initial user, enter the default user name **`admin`** and press Return at the `Password:` prompt. The first time you access the command line interface using the Admin level, there is no password.

CAUTION: *Your system is open to anyone until you set a password for the Admin level. Use the* **`system password`** *command to set a password immediately you gain access.*

We recommend that when you have accessed the unit, you change the default passwords for the other user levels (if you have not already done so) by logging in as the different user levels.

Logging On

At subsequent logins, enter your user name and then your password (at the `Password:` prompt). You must enter your user name and password correctly before you can continue with your management session.

If you have logged on correctly, the initial menu appears. If you have not logged on correctly, the message `Incorrect password` appears and the login sequence starts again.

Default User Names and Passwords

Table 4 shows the default users that can access the unit and their level of access. We recommend that setting a password is the first task you carry out on the unit. Setting a password prevents unauthorized management access to the unit or stack.

Table 4 Default Users

User Name	Default Password	Access Level
monitor	monitor	Monitor — this user can view but not change any operational parameters
manager	manager	Manager — this user can access and change the operational parameters but not special/security features
security	security	Security — this user can access and change all manageable parameters
admin	(none)	Security

Logging Off

At the top level of the command line interface, if you enter the command **`logout`** the management session is terminated.

Automatic Logout

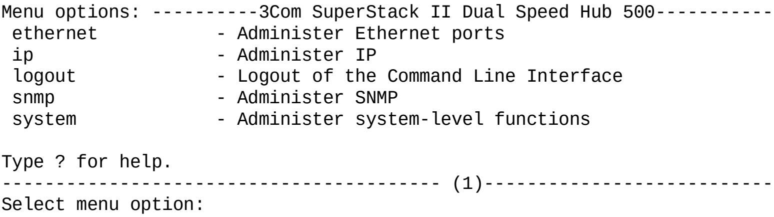
As a security measure, a management session will be terminated if there is a period of inactivity lasting longer than 30 minutes.

After the session has terminated, the first key that you press returns you to the login prompt.

Using the Menus

When you log on to the command line interface correctly, the top-level menu is displayed, as shown in Figure 5. The unit description, unit name and unit number are shown (`Dual Speed Hub 500` and `Marketing (1)` in this example).

Figure 5 Top-level Menu



```
Menu options: ----------3Com SuperStack II Dual Speed Hub 500-----------
 ethernet             - Administer Ethernet ports
 ip                   - Administer IP
 logout               - Logout of the Command Line Interface
 snmp                 - Administer SNMP
 system               - Administer system-level functions

Type ? for help.
----------------------------------------- (1)--------------------------
Select menu option:
```

If the stack is connected and configured as recommended in the user guide that accompanies the unit, the bottom unit in the stack is unit number 1, the next unit up is unit number 2, and so on.

Use the command line interface by selecting options from this menu and from the others below it. Each menu option is accompanied by a brief description of what that option does.

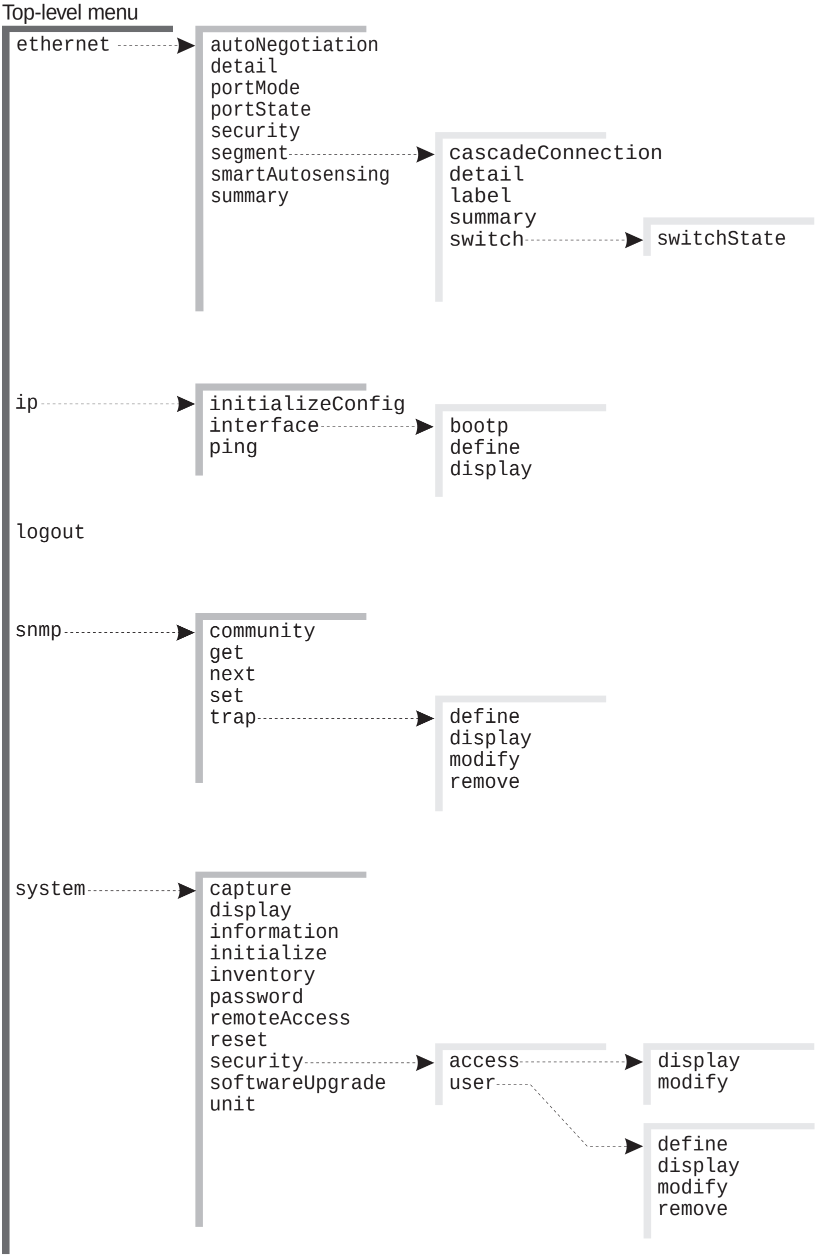
Menu Structure

Figure 6 shows the menu/command structure for the command line interface.

A number of new commands and their hierarchies were introduced with version 2 agent. These are:

- The **`ethernet`** commands — **`autoNegotiation`**, **`detail`**, **`portMode`**, **`security`**, **`segment`** and **`smartAutosensing`**
- All **`snmp`** commands
- The **`system`** commands — **`information`** and **`security`**

Figure 6 Command Line Interface Menu Structure



From the top-level menu, you can access four sub-menus:

- **Ethernet Menu** — From here you can enable or disable ports, view status information about them, and configure Smart auto-sensing for the entire stack.
- **IP Menu** — From here, you can configure IP parameters and PING other devices in your network. You can also reset all IP information back to factory defaults.
- **SNMP** — From here, you can set the community string for users on all units in a stack, and configure trap parameters.
- **System Menu** — From here, you can view system configuration, configure unit parameters, change your password, reset the stack and initialize the stack.

Navigating the Menus and Entering Commands

You can navigate the menus using any of the following methods:

- Following the menu hierarchy — at the `Select menu option:` prompt, type your selected menu name and press Return. The screen changes to show the next level of menus available or the list of commands available within your selected menu.
- Entering multiple menu names on the same line — if you are familiar with the menu structure you can enter the complete command path on the same line at the `Select menu option:` prompt. For example, to display the system configuration, the command line interface would read:

  ```
  Select menu option: system display
  ```

- Abbreviated commands — for quick navigation of the menus, you need only enter enough characters to uniquely identify the menu you want at the prompt. For example, to display system configuration, the command line interface would read:

  ```
  Select menu option: sy di
  ```

As you navigate through the menus, the prompt changes to display your current position in the hierarchy. For example, if you are in the system menu, ready to enter your next option, the prompt reads:

```
Select menu option (system):
```

Entering Commands

When you reach the menu level containing the specific command you want to enter, you are prompted for a command name. Commands can also be entered at the end of the menu string. Where applicable, default values for commands are shown in parentheses after the prompt. If you press Return for a command with such a value, the unit continues to use that value.

Returning to the Previous Menu

You can return to the previous menu, by entering **q** at the prompt.

Returning to the Top-level Menu

You can return to the top-level menu by pressing Esc.

Obtaining Help

You can get help at any time by entering **?** at the prompt.

Quick Guide to the Commands

Table 5 lists all the commands available below the top level headings.

Table 5 Command Line Interface Commands

Command	What does it do?	Described on...
Ethernet Menu		
`autoNegotiation`	Enables and disables auto-negotiation for ports on the current unit in the stack.	page 56
`detail`	Displays detailed information and statistics about a single Ethernet port.	page 56
`portMode`	Specifies the speed of ports on the current Hub in the stack.	page 59
`portState`	Enables and disables ports on the current unit in the stack.	page 54
`security`	Allows you to set security on a port.	page 59

(continued)

Table 5 Command Line Interface Commands (continued)

Command		What does it do?	Described on...
segment	**cascade-Connection**	Connects or disconnects a segment from the cascade unit.	page 64
	detail	Displays detailed information and statistics about a single Ethernet segment.	page 61
	label	Allows you to set the name (label) of an Ethernet segment.	page 61
	summary	Displays summary information about a single Ethernet segment or all segments.	page 63
	switch switchState	Allows you to disable the segment switch between segments.	page 65
smartAutosensing		Enables and disables Smart auto-sensing for the stack.	page 65
summary		Displays information about the ports on the current unit in the stack.	page 54
IP Menu			
initializeConfig		Allows you to reset the IP configuration back to factory defaults. This command operates on the entire stack.	page 68
interface	**bootp**	Enables and disables BOOTP for the current unit in the stack.	page 52
	define	Specifies IP and SLIP information for the current unit in the stack.	page 51
	display	Displays IP and SLIP information for the current unit in the stack.	page 52
ping		Allows you to PING other devices on your network.	page 68
SNMP Menu			
community		Allows you to set the SNMP community string for all units in a stack.	page 70
get		Performs an SNMP GET instruction, that allows you to retrieve values of SNMP objects from the stack.	page 72
next		Performs an SNMP GETNEXT instruction, that allows you to specify an SNMP object and then retrieve the next few SNMP objects from the stack.	page 72

(continued)

Table 5 Command Line Interface Commands (continued)

Command		**What does it do?**	**Described on...**
`set`		Performs an SNMP SET instruction, that allows you to modify the value of an SNMP object in the stack.	page 72
`trap`	**`define`**	Specifies the trap destination details for the stack.	page 70
	`display`	Displays the details of the current trap destinations for the stack.	page 71
	`modify`	Modifies trap destination details for the stack.	page 71
	`remove`	Removes trap destination details from the stack.	page 72
System Menu			
`capture`		Enables and disables RMON Filter capture.	page 67
`display`		Displays configuration information for the current unit in the stack.	page 52
`information`		Allows you to set system name, location and contact.	page 47
`initialize`		Resets the unit to its default settings.	page 66
`inventory`		Lists the units in the stack.	page 53
`password`		Specifies the password for the current user.	page 46
`remoteAccess`		Enables and disables all forms of remote access to the stack.	page 67
`reset`		Simulates powering off and powering on the stack.	page 65
`security`	**`access display`**	Displays the access rights for all access levels in the stack.	page 49
	`access modify`	Modifies the access rights of the access levels in the stack.	page 49
	`user define`	Specifies the user details for the stack.	page 47
	`user display`	Displays the user details for the stack.	page 48
	`user modify`	Modifies user details for the stack.	page 48
	`user remove`	Removes user details from the stack.	page 49
`softwareUpgrade`		Upgrades the management agent with a new version.	page 69

(continued)

Table 5 Command Line Interface Commands (continued)

Command	What does it do?	Described on...
`unit`	Moves the focus of the command line interface to another unit in the stack.	page 50

Commands

The remaining sections in this chapter describe the management functions that can be carried out from the command line interface.

Changing the Password

We recommend that setting a password is the first task you carry out on the unit. Setting a password prevents unauthorized management access to the unit or stack.

ℹ *If you forget your password while logged out of the hub, refer to "Solving Problems With the Command Line Interface" on page 106.*

To set a new password or change an existing password:

1 At the top-level menu, enter:

```
system password
```

2 You are prompted for your old password:

```
Old password:
```

If there is no current password, press Return without entering any text. If you already have a password set up, then enter the password.

3 The prompt changes to show:

```
Enter new password:
```

Enter your new password. The prompt asks you to confirm your new password by entering it again.

The command line interface displays a message to tell you that your password has successfully changed.

Configuring Other System Parameters

You can display and change information about the Hub units in the stack, or the stack as a whole, using the commands on the System menu.

Setting System Information

These commands allow you to set a system name, contact and location for all units in a stack.

At the Top-level menu enter:

`system information`

The CLI prompt shows you the current system information in square parentheses, and allows you to set the new information:

```
Enter system name   [Marketing]: Tech Pubs
Enter system        [John Smith]: Theta
Enter system        [Marketing]: Marketing
```

Specifying User Details

You can specify user details for the stack using the **`define`** command on the System/Security/User menu.

To specify user details for the stack:

1. From the Top-level menu, enter:

   `system security user define`

   The following prompt is displayed:

   `Enter a new user name:`

2. Enter a name for the new user.

   The following prompt is displayed:

   ```
   Enter the access level (monitor,manager,security)
   [security]:
   ```

3. Enter an access level for the new user.

   The following prompt is displayed:

   `Enter the password:`

4. Enter a password for the new user.

   The following prompt is displayed:

   `Re-enter the password:`

5. Enter the password for the new user again.

   The following prompt is displayed:

```
Enter the community string [<user>]:
```

6 Enter a community string for the new user.

Displaying User Details

You can display the user details for the stack using the **`display`** command on the System/Security/User menu.

It is recommended that all of the default passwords are changed.

To display the user details for the stack:

- From the Top-level menu, enter:

  `system security user display`

  The user details are displayed.

An example of the details is shown below:

```
Name            Access Level    Community String
admin           security        admin
manager         manager         manager
monitor         monitor         monitor
security        security        security
```

Modifying User Details

You can modify user details for the stack using the **`modify`** command on the System/Security/User menu.

To modify user details for the stack:

1 From the Top-level menu, enter:

`system security user modify`

The following prompt is displayed:

```
Enter the user name:
```

2 Enter the name of the user to be modified.

The following prompt is displayed:

```
Enter the password:
```

3 Enter a password for the user.

The following prompt is displayed:

```
Re-enter the password:
```

4 Enter the password for the user again. The following prompt is displayed:

```
Enter the community string [<user>]:
```

5 Enter a community string for the user.

Removing User Details

You can remove user details from the stack using the **`remove`** command on the System/Security/User menu.

To remove user details from the stack:

1 From the Top-level menu, enter:

```
system security user remove
```

The following prompt is displayed:

```
Enter the user name (<users>,all):
```

2 Enter the name of the user that is to have its details removed, or enter **`all`** to remove the details of all users (except default users).

Displaying Access Rights

You can display the access rights for all access levels in the stack using the **`display`** command on the System/Security/Access menu.

To display the access rights for the stack:

- From the Top-level menu, enter:

  ```
  system security access display
  ```

  The access rights are displayed.

An example of the access rights information is shown below:

```
Access Level  SNMP      Console    Telnet     Web
monitor       enable    enable     enable     enable
manager       enable    enable     enable     enable
security      enable    enable     enable     enable
```

Modifying Access Rights

You can modify access rights for the access levels in the stack using the **`modify`** command on the System/Security/Access menu.

To modify the access rights for the stack:

1 From the Top-level menu, enter:

```
system security access modify
```

The following prompt is displayed:

```
Enter access level (monitor,manager,security):
```

2 Enter the access level to be modified. The following prompt is displayed:

```
Enter new value for SNMP (enable,disable) [enable]:
```

3 Enter **enable** if the access level allows SNMP management, or **disable** if it does not. The following prompt is displayed:

```
Enter new value for console (enable,disable) [enable]:
```

4 Enter **enable** if the access level allows management through a console port of the stack, or **disable** if it does not. The following prompt is displayed:

```
Enter new value for telnet (enable,disable) [enable]:
```

5 Enter **enable** if the access level allows telnet management, or **disable** if it does not. The following prompt is displayed:

```
Enter new value for web (enable,disable) [enable]:
```

Enter **enable** if the access level allows web management, or **disable** if it does not.

Configuring Another Unit in the Stack

Many commands in the command line interface perform actions on a specific unit in the stack (the unit you are managing). You can move the focus of the command line interface to another unit easily.

To configure another unit in the stack:

1 At the top-level menu, enter:

```
system unit
```

You are prompted for the unit's number:

```
Select unit:
```

2 Enter the unit's number.

If the stack is correctly connected and configured as recommended, the bottom unit in the stack is unit number 1, the next unit is unit number 2, and so on.

When you have finished configuring the unit, simply log out to return to the previous unit.

Configuring the Unit's IP Information

Before you can manage the unit or stack over the network, you must assign it an IP address and subnet mask. You may also need to enter a default gateway (sometimes known as the default router) address. The default router is the router (if you have one) that is used by the stack to communicate with other networks. For serial management, you may need to configure the SLIP address and SLIP subnet mask.

If you have no previous knowledge of IP, refer to "IP Addresses" on page 30. If you change any of these values, you may need to re-access the hub using the new values.

The IP information is stored in the unit but can be used to access the whole stack.

If you enable BOOTP for the unit and there is a BOOTP server on your network, the server can automatically allocate an IP address, subnet mask and default router address to the unit. For information on how to use your BOOTP server, refer to the documentation that accompanies it.

Configuring the IP Information

To enter new IP settings:

1. At the top-level menu, enter:

   ```
   ip interface define
   ```

2. You are prompted for the unit's IP address:

   ```
   Enter IP address [0.0.0.0]:
   ```

   Enter a valid IP address for the unit.

3. You are prompted for the unit's subnet mask:

   ```
   Enter subnet mask [255.255.255.0]:
   ```

   Enter a subnet mask.

4. You are prompted for a default router address:

   ```
   Enter default gateway [0.0.0.0]:
   ```

   Enter a default gateway address or press Return if it is not required.

5. You are prompted for a SLIP address:

   ```
   Enter SLIP address [192.168.101.1]:
   ```

Enter a SLIP address or press Return if it is not required.

6 Finally, you are prompted for a SLIP subnet mask:

```
Enter SLIP subnet mask [255.255.255.0]:
```

Enter a SLIP subnet mask or press Return if it is not required.

Any changes that you make will take effect after a few seconds. You do not need to reset the stack.

Enabling and Disabling BOOTP

To enter new IP settings:

1 At the top-level menu, enter:

```
ip interface bootp
```

2 You are prompted for the unit's new BOOTP state:

```
Enter new value (enabled, disabled) [enabled]:
```

Enable or disable BOOTP as required.

Viewing the Configuration

You can use the **display** command to show current configuration information for your unit or stack.

Displaying the IP Information

At the top-level menu, enter:

```
ip interface display
```

The command line interface displays the IP address, subnet mask, default router address, SLIP address and SLIP subnet mask for the unit.

Displaying the Administration Information

At the top-level menu, enter:

```
system display
```

The command line interface displays information similar to this example:

```
3Com Dual Speed Hub 500 (3C16611)
Unit Name: Marketing
Location: Top floor
Contact: James
```

```
Time since reset: 2 days, 3 hours, 10 minutes
Operational Version: 2.14
Hardware Version: 2.00
Boot Version: 1.00
MAC Address : 08:00:4e:4f:9c:42
Product Number : 3C16611
Serial Number: 2103332
```

In the example above, you will see the term 'Operational Version". This is the same as the software agent version. It is diffentiated to avoid confusion with the BOOT version.

This information is in the unit's MIB (Management Information Base) and is read-only. You can change the Unit name, Location and Contact using the web interface.

If a problem occurs and you need advice from your support representative, you may be asked for some of the information shown on this screen.

Displaying Summary Information for the Stack

The **`inventory`** command allows you to list the units in the stack.

At the top-level menu, enter:

```
system inventory
```

The command line interface displays the position, description, name and state of the units in the stack.

Where:

- **Position** — The position of the unit in the stack; if the stack is correctly connected and configured as recommended, the bottom unit in the stack is unit number 1, the next unit is unit number 2, and so on.
- **Description** — The type of unit.
- **Unit Name** — The name that you have assigned to the unit.
- **State** — The current operating status of the unit:
  - *Unit Operational* — Indicates that the unit is operating normally.
  - *Unit Loading* — Indicates that there is a process taking place, for example a software upgrade.

Configuring the Unit's Ports

You can view and change information about the ports on the unit using the command line interface. You can:

- Enable and disable the ports.
- View information about the status of the ports.

To view and change information about the ports on another unit in the stack, use the **unit** command to change unit; refer to "Configuring Another Unit in the Stack" on page 50.

Enabling and Disabling the Ports

By default, all ports on the unit are enabled. To prevent unauthorized access to the unit, we recommend that you disable any ports that are not being used.

To configure a port:

1 At the top-level menu, enter:

```
ethernet portState
```

2 You are prompted for the port number:

```
Select Ethernet port (1-26):
```

Enter the number of the port (ports 25 and 26 are the transceiver module ports).

3 Enable or disable the port as required.

Displaying the Port Status

To view the port status information:

1 At the top-level menu, enter:

```
ethernet summary
```

2 You are prompted for the port number:

```
Select Ethernet port (1-26,all) [all]:
```

Enter the number of the port (ports 25 and 26 are the transceiver module ports), or enter **all** if you wish to view all of the ports.

The command line interface displays the port status, including the number of packets, octets and errors it has received, similar to this example:

```
 Port      State      RX Packets    RX Octets    Errors
   3      enabled       460380       487234        0
```

If there is a high number of errors, it could indicate that there is faulty equipment somewhere on the network segments that are connected to the ports, or that the network is badly configured.

Displaying and Changing Port Information

From the Ethernet sub-menu you can display information about your network since the Hub was last reset, initialized or powered off/on. The new commands allow you to:

- Enable and disable auto-negotiation for Ethernet ports on the Hub
- Display statistical information about Ethernet ports on the Hub
- Specify the speed of Ethernet ports on the Hub
- Enable and disable security for Ethernet ports on the Hub

Enabling and Disabling Auto-negotiation

Auto-negotiation is a system that allows the Hub to automatically detect the speed of twisted pair links, and thereby set the speed of its twisted pair ports. If auto-negotiation is enabled on a 10BASE-T/100BASE-TX port, the speed of the link is automatically detected and set accordingly.

You can enable and disable auto-negotiation for Ethernet ports on the Hub using the **`autoNegotiation`** command on the Ethernet menu.

1 At the Top-level menu, enter:

```
ethernet autoNegotiation
```

The following prompt is displayed:

```
Select Ethernet port (1-24):
```

2 Enter the number of the port to have auto-negotiation enabled or disabled.

The following prompt is displayed:

```
Enter new value (enable,disable) [enable]:
```

3 Enter **`enable`** or **`disable`**.

Fiber ports and Transceiver Module ports are not auto-negotiating. If the port is one of these ports, auto-negotiation cannot be enabled.

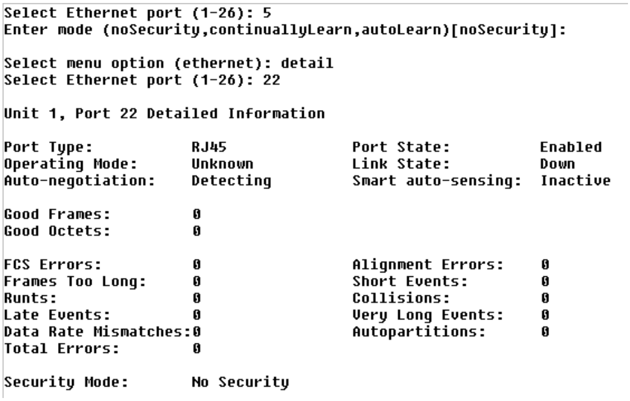
If auto-negotiation is disabled, the speed of the port is set using the **`portMode`** *command. For more information, see "Specifying the Speed of a Port" on page 59.*

Ethernet Port Statistics

You can display detailed information about a single Ethernet port by entering the following:

```
ethernet detail
```

The command line interface shows a screen of information similar to the following:



```
Select Ethernet port (1-26): 5
Enter mode (noSecurity,continuallyLearn,autoLearn)[noSecurity]:

Select menu option (ethernet): detail
Select Ethernet port (1-26): 22

Unit 1, Port 22 Detailed Information

Port Type:           RJ45              Port State:          Enabled
Operating Mode:      Unknown           Link State:          Down
Auto-negotiation:    Detecting         Smart auto-sensing:  Inactive

Good Frames:         0
Good Octets:         0

FCS Errors:          0                 Alignment Errors:    0
Frames Too Long:     0                 Short Events:        0
Runts:               0                 Collisions:          0
Late Events:         0                 Very Long Events:    0
Data Rate Mismatches:0                 Autopartitions:      0
Total Errors:        0

Security Mode:       No Security
```

The screen shows the following statistics:

- `Good Frames` — This is the total number of frames with no errors seen at the port. Examining this statistic regularly can help you monitor your network's overall performance. For example unusual increases in traffic rate may indicate a potential problem.
- `Good Octets` — This field shows the total number of octets (bytes) received as part of Good Frames at the port. The total includes the header, data and FCS (Frame Check Sequence) 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.
- `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). If the number of FCS errors is a large 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.
- `Alignment Errors` — The alignment errors count is the number of frames that are not a whole number of octets in length and do not pass the FCS check. 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.

- `Frames Too Long` — These are frames that exceed the maximum size for Ethernet 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.
- `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.
- `Runts` — Runt frames are frames that are smaller than the minimum frame size defined for Ethernet frames, but are longer than Short Events. Runts may occur as the result of collision, and will be propogated around the network. This is a normal part of Ethernet operation and is not an error.
- `Collisions` — Collisions are a normal part of Ethernet 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.
- `Late Events` — A late event is an ‘out-of-window’ collision, which may occur if you have a network that exceeds the maximum size (defined by IEEE Ethernet standards). A late event is also counted as a collision.
- `Very Long Events` — The very long event statistic shows how many times the hub has had to protect against jabbers 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.
- `Data Rate Mismatches` — These are frames received at the port whose timing was outside the permitted frequency range. This may indicate non-compliant or faulty devices on your network.
- `Autopartitions` — This is the number of times the port has automatically partitioned. Autopartitioning occurs when excessive (more than 64) consecutive collisions occur at a single port.

- `Total Errors` — This number should be a small proportion of the Good Frames number. It is the sum of the following errors seen at the port:
    - FCS Errors
    - FCS Alignment Errors
    - Short Events
    - Frames Too Long
    - Very Long Events
    - Data Rate Mismatches
    - Late Events

Specifying the Speed of a Port

You can specify the speed of Ethernet ports on the Hub using the **`portMode`** command on the Ethernet menu.

To specify the speed of a port:

1 At the Top-level menu, enter:

```
ethernet portMode
```

The following prompt is displayed:

```
Select Ethernet port (1-24):
```

2 Enter the speed required:

```
Enter new value (100half,10half): 10half
```

Port speeds specified using the **`portMode`** *command do not take effect until auto-negotiation is disabled on the port. For more information, see “Enabling and Disabling Auto-negotiation” on page 59.*

Port Security Feature

You can enable and disable security features on an Ethernet port using the **`security`** command on the Ethernet menu. These security features are Disconnect Unauthorised Device (DUD) and Need to Know (NTK).

Disconnect Unauthorised Device (DUD) If a packet address is seen on a port that is not known by the Hub (it has not been learnt), that port will be disabled.

Need to Know (NTK) In normal Hub operation, packets received are sent to all ports irrespective of the packet destination address. With NTK enabled, the Hub sends a packet to its destination address, but will scramble it when sending the packet to all the other secure ports.

1 To enable and disable DUD and NTK using the command line interface, at the Top-level menu enter:

```
ethernet security
```

The following prompt is displayed:

```
Select Ethernet port (1-26): 5
```

2 You are then prompted to enter the security operation mode required:

```
Enter mode (noSecurity, continuallyLearn, autoLearn)
[noSecurity]:
```

a If you enter **noSecurity**, all security features will be disabled.

b If you enter **continuallyLearn**, the following prompt is displayed:

```
Enter the number of authorized addresses (0–33) [1]:
```

The number of authorized addresses you enter is the number of devices allowed to transmit or receive on that port. For example, if you enter **3**, the Hub will learn three addresses at any one time for the specified port. When a new address is received, the most recent three addresses received will be remembered, and the oldest one dropped.

c If you enter **autoLearn**, the following prompt is displayed:

```
Enter the number of authorized addresses (0–33) [1]:
```

The number of authorized addresses you enter is the number of devices allowed to transmit or receive on that port. For example, if you enter **3**, the Hub will remember three addresses *only* for the specified port. Any new addresses will not be allowed to transmit or receive from this port.

3 If you have entered **continuallyLearn** or **autoLearn** the following prompt is displayed:

```
Need to Know Mode (enable, disable) [disable]:
```

a If you have entered **continuallyLearn** enable or disable NTK as required.

b If you have entered **`autoLearn`**, enable or disable NTK as required. You are then prompted with the following:

```
Enter Disconnect Unauthorized Device mode
(enable,disable) [disable]:
```

Enable or disable DUD as required.

Ethernet Segment Management

Naming an Ethernet Segment

The **`label`** command allows you to create a name (or *label*) for a segment.

1 At the Top-level menu enter:

```
ethernet segment label
```

2 You are prompted to enter the number of the Ethernet segment:

```
Select Ethernet segment (10,100) : 10
```

3 You are then prompted to enter a new name for the segment:

```
Enter new value [Seg-2] : Sales
```

Ethernet Segment Statistics

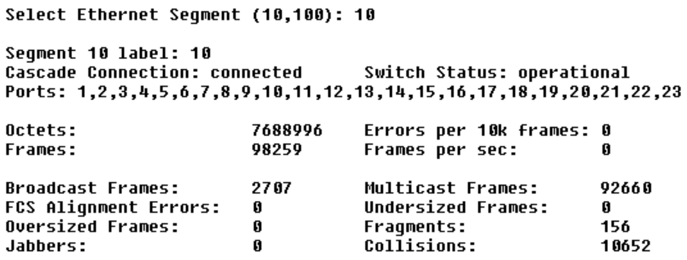
You can display detailed information about a single Ethernet segment since the last reset.

1 At the Top-level menu enter the following:

```
ethernet segment detail
```

2 You are then prompted to enter the number of the segment.

The command line interface shows a screen of information similar to the following:



```
Select Ethernet Segment (10,100): 10

Segment 10 label: 10
Cascade Connection: connected      Switch Status: operational
Ports: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23

Octets:                  7688996    Errors per 10k frames: 0
Frames:                  98259      Frames per sec:        0

Broadcast Frames:        2707       Multicast Frames:      92660
FCS Alignment Errors:    0          Undersized Frames:     0
Oversized Frames:        0          Fragments:             156
Jabbers:                 0          Collisions:            10652
```

The screen shows the following statistics:

- `Octets` — This is the number of octets transmitted/received on this segment. This calculation includes the MAC header and FCS, but excludes preamble/Start-of-Frame Delimiter.
- `Frames` — This is the total number of frames since last reset. Examining the statistic regularly can help you monitor network traffic.
- `Broadcast Frames` — This is the total number of broadcast frames seen on the segment. Broadcast frames are frames that are addressed to all MAC addresses (that is, all devices) in a segment. A high level of broadcast frames can adversely affect network performance.
- Errors per 10K Frames — This is the number of errors seen on the segment per 10,000 frames, sampled every 60 seconds.
- `Frames per second` — This is the average number of frames seen per second at the segment, sampled every 60 seconds.
- `Multicast Frames` — This is the total number of multicast frames seen at the segment. A multicast frame is one that is addressed to a group of MAC addresses (that is, several devices) on the network. A high level of multicast frames can adversely affect network performance.
- `FCS Alignment Errors` — The alignment errors count is the number of frames that are not an integral number of octets in length and do not pass the FCS check. Alignment errors may be caused by a fault at the transmitting device. Check transceiver or adapter cards of devices connected to this segment. If this does not solve the problem, check cables and connections for damage.
- `Undersized Frames` — The total number of error packets seen on this segment, which are smaller than the minimum size defined for packets (defined by IEEE Ethernet standards). Undersize packets may indicate externally generated noise causing problems on the network. Check the cabling routing and re-route any cabling which may be affected by external noise sources.
- `Oversized Frames` — The total number of packets seen on this segment that exceed the maximum length defined for packets (1518 octets). If you see a high number of oversize packets on your network segment, you need to isolate the source

of these packets and examine the transceiver or adapter card at the device. Some protocols may generate these packets.

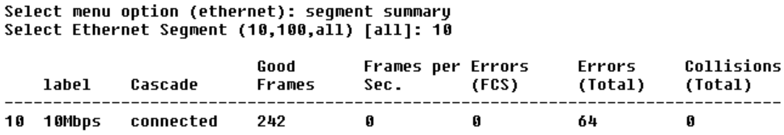
- `Fragments` — The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).
- `Jabbers` — The total number of packets received on this segment that were longer than 8,000 octets (excluding framing bits, but including FCS octets). Jabber is the uncontrolled transmission of oversized packets to the network by a faulty device.
- `Collisions` — An estimate of the total number of collisions that occurred when transmitting on the segment.

Displaying Ethernet Segment Summary Information

You can use the **`summary`** command to display summary information about a single Ethernet segment or all segments on a Hub since last reset. From the Top-level menu enter:

`ethernet segment summary`

The command line interface shows a screen of information similar to the following:



```
Select menu option (ethernet): segment summary
Select Ethernet Segment (10,100,all) [all]: 10

                          Good        Frames per Errors      Errors     Collisions
    label    Cascade      Frames      Sec.       (FCS)       (Total)    (Total)
--------------------------------------------------------------------------------
10  10Mbps   connected    242         0          0           64         0
```

The statistics that are displayed are accumulated over the time interval since the last reset, initialization or power-off/on cycle. The `Errors (Total)` statistic is the sum of the following errors:

- FCS Alignment Errors
- Undersized Packets
- Oversized Packets
- Fragments
- Jabbers

Managing the Ethernet Segment Cascade Connection

When you connect 10Mbps and 100Mbps equipment to the unit, the ports are automatically connected to the relevant segment. The segment switch joins the 10Mbps and 100Mbps segments so that all of the equipment connected to the segments can communicate.

By default, the Dual Speed Hub 500 is configured so that all of its segments are connected, and its switch is in 'AutoConfigure' mode. This ensures that all equipment connected to the stack can communicate through the stack. Only alter these settings if you want to alter the operation of the unit's switch. See "Configuring the Switch Between Segments" below.

This command allows you to connect or isolate a labeled segment to/from the cascaded segment of the same speed connected to other units in the stack.

Isolating the segment means that traffic received by the unit is not passed on to other units in the stack.

Traffic may be passed on by the segment of the other speed, if that segment is not isolated and the unit's segment switch is operational.

If you have a Dual Speed Hub 500 with a serial number less than ***0600/00000000000****, upgrading the software to version 2.1x or above will not give you support for segment isolation.*

1 At the Top-level menu enter the following:

```
ethernet segment cascadeConnection
```

You are then prompted to enter the label of the segment.

```
Enter segment label:
```

2 Enter the label of the segment to be managed.

You are then prompted for the management operation.

```
Change the cascadeConnection (connect, isolate)
[connect]
```

Enter the new state.

Configuring the Switch Between Segments

You can enable or disable the segment switch between segments using the **`ethernet segment switch switchState`** command.

1 At the Top-level menu enter:

```
ethernet segment switch switchState
```

The following prompt is displayed:

```
Enter new value (autoConfigure,disabled)
[autoConfigure]:
```

2 Enter the new value as required.

CAUTION: *If you are managing any unit of a stack over a 100Mbps connection, disabling the segment switch on the bottom unit will prevent further management of the unit. If you do lose management in this way, follow the procedure below.*

Management Recovery Procedure To recover management connection over the 100Mbps segment, enter the following into the Top-level menu of the local command line interface (on the bottom unit):

```
ethernet segment switch switchState
```

The following prompt is displayed:

```
Enter new value (autoConfigure,disabled)
[autoConfigure]:
```

Enter the new value as required.

Enabling and Disabling Smart Auto-sensing

Smart auto-sensing checks the quality of any new 100Mbps connection made to the stack. If the connection is unsuitable at 100Mbps, it automatically downgrades the connection to 10Mbps. By default, Smart auto-sensing is enabled for the stack. For more information on Smart auto-sensing, refer to "Smart Auto-sensing Feature" on page 16.

To configure Smart auto-sensing:

1 At the top-level menu, enter:

```
ethernet smartAutosensing
```

2 You are prompted for the stack's new Smart auto-sensing state:

```
Enter new value (enable, disable) [enable]:
```

Enable or disable Smart auto-sensing as required.

Resetting the Stack

Resetting the stack simulates powering off and powering on the stack. You may want to do this if you want to reset the stack's statistics counters.

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

To reset the stack:

1 At the top-level menu, enter:

```
system reset
```

2 The command line interface asks you to confirm the reset. Enter **y** if you wish to proceed, or **n** if you want to stop the reset.

During a reset, you are unable to communicate with the stack. After the reset, press Return twice to restore communication (if required). The reset process takes about 10 seconds.

Initializing the Stack

Initializing the stack causes it to return to its factory default settings, and the stack is reset. You may want to do this if the stack has been previously used in a different part of your network, and its settings are incorrect for its new environment.

CAUTION: *Initializing the stack removes all configuration information including resilient links and passwords (you will need to use the default password to re-access the stack). However, IP, SLIP and default router information is retained to ensure you can continue management communication with the stack over the network. If you have any resilient links set up for the stack, you may experience network loops after the initialize.*

To initialize the stack:

1 At the top-level menu, enter:

```
system initialize
```

2 The command line interface asks you to confirm the initialize. Enter **y** if you wish to proceed, or **n** if you want to stop the initialize.

During an initialize, you are unable to communicate with the stack. After the initialize, press Return twice to restore communication (if required). The initialize process takes about 10 seconds.

Enabling and Disabling Remote Access to the Stack

As a security measure, you can enable or disable remote access to the management software of the stack:

- When remote access is enabled, users can access the management software using all management methods.
- When remote access is disabled, users cannot access the management software over the network. This includes remote access using:
  - The command line interface (over Telnet)
  - The web interface
  - An SNMP network management application
  - An RMON management application

To configure remote access:

1 At the top-level menu, enter:

```
system remoteAccess
```

2 Enable or disable remote access as required.

Enabling and Disabling RMON Filter Capture

You can enable or disable RMON Filter capture. By default this is enabled. You may wish to disable this if you have no requirement to perform RMON packet monitoring and wish to increase the security of your network.

RMON Filter capture is enabled and disabled on a per unit basis. If you want to change Filter capture for the whole stack, you must perform the command for each unit (accessing each unit in turn).

*If you have a Dual Speed Hub 500 with a serial number less than **0600/00000000000**, upgrading the software to version 2.1x or above will not give you support for the RMON Filter and Capture groups on the 100Mbps segments, which means that you cannot perform RMON Filter Capture for the 100Mbps segments.*

To configure RMON Filter capture:

1 At the top-level menu, enter:

```
system capture
```

2 Enable or disable RMON Filter capture as required.

Using PING to Test the Connections to Other Devices

From the command line interface you can send out a PING request to test that a device on your network can receive and transmit information to the stack. You can use PING to ensure that the stack is installed correctly, and that your network connections are good.

To PING a device:

1 At the top-level menu, enter:

```
ip ping
```

2 You are prompted for the device's IP address:

```
Enter destination IP address:
```

Enter the IP address of the device.

The command line interface transmits a single PING request to the device. It then displays a message telling you if it received a response, for example:

```
Starting ping, resolution of displayed time is
10 milli-sec
Response from 192.168.100.30: 1 router hop. time = 10ms
```

Resetting the IP Configuration

You can reset the IP configuration for the whole stack back to factory defaults.

To do this:

1 At the top-level menu, enter:

```
ip initializeConfig
```

The following warning is displayed:

```
WARNING: This change will lock out all SNMP, Telnet and
Web based management access.

Do you wish to continue (yes/no) [no]:
```

2 Enter **`yes`** to reset the IP configuration.

Upgrading the Management Software

When 3Com issues a new version of the management software agent for the Dual Speed Hub 500, you can upgrade the units in your stack.

You must copy the new management software agent into the appropriate directory on a TFTP server (use the directory that the TFTP server has been configured to look in). For information on how to use your TFTP server, refer to the documentation that accompanies it.

During a software upgrade, you are unable to communicate with the stack. After a successful upgrade, the stack resets itself and communication is restored. The upgrade process may take up to 5 minutes for each unit.

When you upgrade a stack, the new management software is stored in each unit. If you add a unit that is running a different version of management software, you must upgrade the unit to ensure that all of the units have the same functionality.

To upgrade the management software for the stack:

1 At the top-level menu, enter:

```
system softwareUpgrade
```

2 You are prompted for the TFTP server's IP address:

```
TFTP Server Address [0.0.0.0]:
```

Enter the IP address of the TFTP server that contains the new management software agent.

3 You are prompted for the file name of the new management software agent:

```
File Name [DSH01_01.bin]:
```

The file name format is **`DSH`*`xx_yy`*`.bin`**, where ***`xx_yy`*** is the version of agent software, for example **`DSH02_00.bin`**.

The command line interface starts the software upgrade.

A power interrupt during the software upgrade may cause a corrupted agent image on the hub. If this occurs then subsequent rebooting of the unit will be unsuccessful and the power LED will flash. In this event the software should be updated using the "Serial Update Utility". See Appendix D on page 127 for details.

Displaying and Changing SNMP-related Information

You can display and change SNMP-related information for the stack using the commands on the SNMP menu. These commands allow you to:

- Specify SNMP community strings for the stack
- Specify the trap destination details for the stack
- Display the trap destination details for the stack
- Modify trap destination details for the stack
- Remove trap destination details for the stack
- Perform an SNMP GET instruction on the stack
- Perform an SNMP GETNEXT instruction on the stack
- Perform an SNMP SET instruction on the stack

Specifying SNMP Community Strings

You can specify SNMP community strings for the users defined on the stack using the **`community`** command on the SNMP menu.

To specify the SNMP community strings:

1 At the Top-level menu, enter:

```
snmp community
```

The following prompt is displayed:

```
Enter new community for user '<user>':
```

2 Enter the community string for the user.

3 Repeat step 2 for the other users defined on the stack.

Specifying Trap Destination Details

You can specify the community string and IP address of devices that are to be the destination for traps on your network using the **`define`** command on the SNMP/Trap menu.

To specify the details of a trap destination device:

1 At the Top-level menu, enter:

```
snmp trap define
```

You are then prompted to enter the trap community string:

```
Enter the trap community string [monitor]:
```

2. You are then prompted to enter the trap destination address:

```
Enter the trap destination address:
```

Displaying Trap Destination Details

You can display the community string and IP addresses of the current trap destinations using the **`display`** command on the SNMP/Trap menu.

To display trap destination details, at the Top-level menu, enter:

```
snmp trap display
```

The trap destination details are displayed.

An example of the information is shown below:

```
Index    Community String    Destination Address
1        monitor             192.168.100.1
2        monitor             192.168.100.2
3        monitor             192.168.100.3
4        monitor             192.168.100.4
```

Modifying Trap Destination Details

You can modify the community string and IP address of a current trap destination using the **`modify`** command on the SNMP/Trap menu.

To modify trap destination details:

1. At the Top-level menu, enter:

```
snmp trap modify
```

The following prompt is displayed:

```
Select trap index (1,2,3):
```

2. Enter the index number of the trap destination to be modified.

The following prompt is displayed:

```
Enter the trap community string [monitor]:
```

3. Enter the new community string of the trap destination.

The following prompt is displayed:

```
Enter the trap destination address [<ip address>]:
```

4 Enter the new IP address of the trap destination.

Removing Trap Destination Details

You can remove the details of a current trap destination device using the **`remove`** command on the SNMP/Trap menu.

To remove trap destination details:

1 At the Top-level menu, enter:

`snmp trap remove`

The following prompt is displayed:

```
Select trap index (1,2,3,all):
```

2 Enter the index number of the trap destination device that is to have its details removed, or enter **`all`** to remove all trap destination device details.

Displaying and Setting SNMP Object Values

We have provided a set of very powerful SNMP commands for use by those of wide experience within networking. These commands may be found in the SNMP menu. Their use will be understood by the intended manager.

CAUTION: *If you are not very familiar with SNMP management, you will create problems by attempting to use these commands.*

If you must know how to use them, use the contacts given in the SuperStack II Dual Speed Hub 500 User Guide (DUA1661-0AAA0x).

4 USING THE WEB INTERFACE

This chapter describes how to use the web interface. If you have any problems using the web interface, refer to "Solving Problems With the Web Interface" on page 107.

Accessing the Web Interface

You can access the web interface for the stack either through the console port or over the network. Ensure that your management station has been appropriately set up for your particular management method and that any necessary connections have been made, refer to "Web Interface" on page 35.

If you want to access the web interface through a serial link from a Windows 95 management station (connected to the console port of a unit in the stack), you must use a SLIP driver that sets up SLIP access for web interface management. A suitable SLIP driver (the 3Com serial web utility) is supplied on the CD-ROM that accompanies the management module; refer to Appendix B.

Any number of people can access the web interface over the network, at the same time. There is a password panel to prevent unauthorized management of the stack.

To access the web interface:

1. Start your Web browser.
2. In the browser, select the option for opening a location.
3. In the browser's open location window or area, enter the Web address *URL* (Uniform Resource Locator) for the stack.

   The Web address URL for a stack is in the format:

   http://*nnn.nnn.nnn.nnn/*

Where *nnn.nnn.nnn.nnn* is:

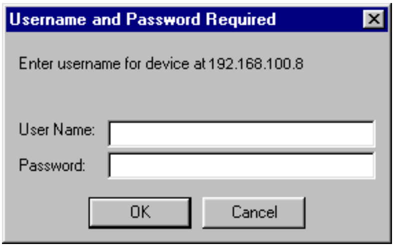
- The SLIP address for the stack, which is '192.168.101.1' by default, if managing through the console port
- The IP address for the stack, if managing over the network

For example, to access a stack with an IP address of '192.168.100.8' you would enter:

```
http://192.168.100.8/
```

4 When the browser has located the stack, a password panel is displayed, as shown in Figure 7. Enter your user name and password as requested.

Figure 7 Password Panel



Username and Password Required

Enter username for device at 192.168.100.8

User Name:

Password:

The user names and passwords are the same as those that you use to access the command line interface. For a list of the user names and the default passwords, refer to "Default User Names and Passwords" on page 38.

We recommend that when you have accessed the stack, you change the default passwords for the user levels (if you have not already done so) by logging in as the different user levels. If you forget your password while logged out of the stack, refer to "Solving Problems With the Web Interface" *on* page 107.

When the correct user name and password have been entered, the web interface appears. You are now ready to manage the stack.

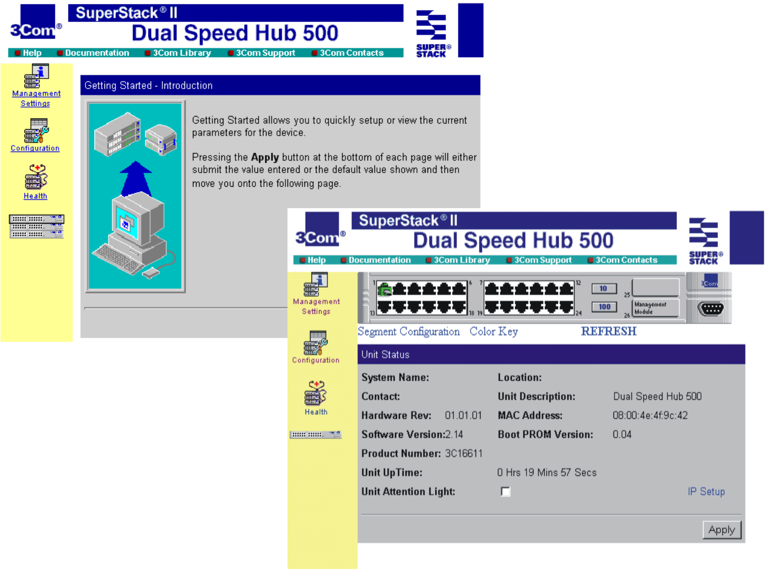
If you are unable the access the web interface, refer to "Solving Problems With the Web Interface" on page 107.

While managing the stack, you can use your Web browser to look at other Web pages or interfaces, and then simply use the back button to re-access the web interface. You do not need to re-enter your user name and password when doing this.

At the start of your management session, the web interface displays one of two pages, as shown in Figure 8:

- **Getting Started page** — This is displayed if it is your first management session from a new management station. For information on how to use the Getting Started pages, refer to "Getting Started" on page 92.
- **Unit Status page** — This is displayed on all other occasions.

Figure 8 The Web Interface



Getting Started - Introduction

Getting Started allows you to quickly setup or view the current parameters for the device.

Pressing the **Apply** button at the bottom of each page will either submit the value entered or the default value shown and then move you onto the following page.

Unit Status

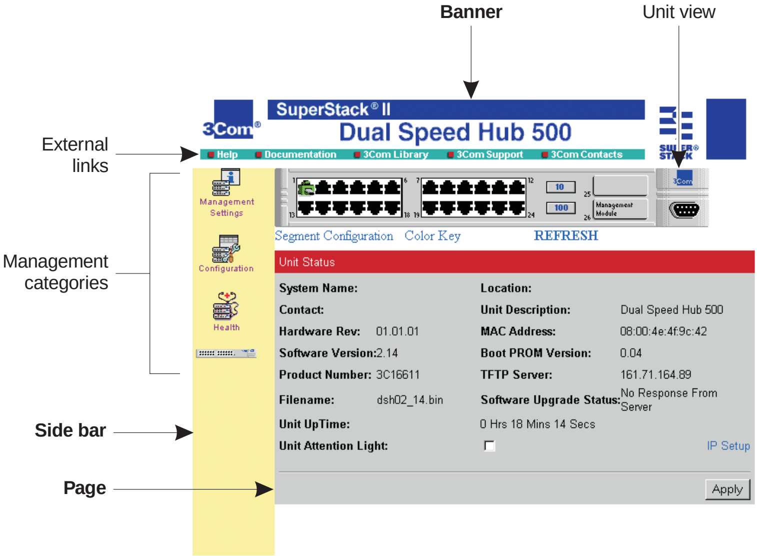
System Name:		**Location:**	
Contact:		**Unit Description:**	Dual Speed Hub 500
Hardware Rev:	01.01.01	**MAC Address:**	08:00:4e:4f:9c:42
Software Version:	2.14	**Boot PROM Version:**	0.04
Product Number:	3C16611		
Unit UpTime:		0 Hrs 19 Mins 57 Secs	
Unit Attention Light:		□	IP Setup

About the Web Interface

The web interface has been designed so that it is easy to use. It is made up of three areas, as shown in Figure 9; the banner, side bar (always displayed) and page (changes to show the different information about the stack).

Some fields are only displayed after a software upgrade failure. These provide information about the software upgrade.

Figure 9 Components of the Web Interface



Unit Status

System Name:

Location:

Contact:

Unit Description: Dual Speed Hub 500

Hardware Rev: 01.01.01

MAC Address: 08:00:4e:4f:9c:42

Software Version:2.14

Boot PROM Version: 0.04

Product Number: 3C16611

TFTP Server: 161.71.164.89

Filename: dsh02_14.bin

Software Upgrade Status: No Response From Server

Unit UpTime: 0 Hrs 18 Mins 14 Secs

Unit Attention Light: □

If you click on the:

- **Management categories** (on the side bar) — The page area changes to show different management information about the stack, for example network addresses and graphs.
- **External links** (on the banner) — The Web browser displays general information which is external to the web interface, for example help and contact information.

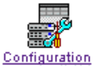
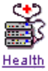
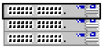
Management Categories

Table 6 shows the management categories that are on the side bar.

Table 6 Management Categories

Management Settings	*Management Settings* — Displays information about the stack's management settings.

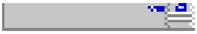
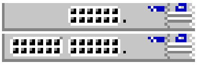
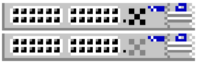
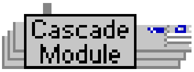
Table 6 Management Categories

	*Configuration* — Displays information about the configuration of some of the stack's features.
	*Health* — Displays statistics for the stack's segments.
	*Stack icon* — Selecting a unit displays information about the unit, including the Unit View and unit information, as shown in Figure 9.

Stack Icon

The stack icon is a representation of the units in the stack. Table 7 shows the different types of units that can be a part of the stack.

Table 7 Units in the Stack Icon

	Manageable Dual Speed Hub 500 (with no access to a management module).
	Managed Dual Speed Hub or PS Hub 40 with: ■ 12 TP ports ■ 24 TP ports
	PS Hub 50 with: ■ Active internal switch ■ Inactive internal switch
	*Cascade Module icon* — A different type of managed unit or stack is connected to the Dual Speed Hub 500 stack by a Cascade Converter Kit. For example, you can use the Dual Speed Hub 500 – Hub 10 Cascade Converter Kit to connect a Hub 10 stack to the Dual Speed Hub 500 stack.

External Links

Table 8 shows the external links that appear on the banner. You can also click on the 3Com logo to display the 3Com Web site.

Table 8 General Icons

Help	Displays the online help system for the web interface.
Documentation	Displays the online version of this user guide.
3Com Library	Displays the 3Com online library from the 3Com Web site.

Table 8 General Icons

3Com Contacts	Displays the 3Com contact page from the 3Com Web site.
3Com Support	Displays the 3Com customer support page from the 3Com Web site.

Before you can use the online help system and online version of this user guide, you may need to copy the files from the CD-ROM onto your management station, refer to "Online Help System and Documentation" on page 82.

If you do not have a connection to the Internet, your Web browser is unable to display 3Com pages from the external links (3Com Library, 3Com Contacts, 3Com Support).

Page Components

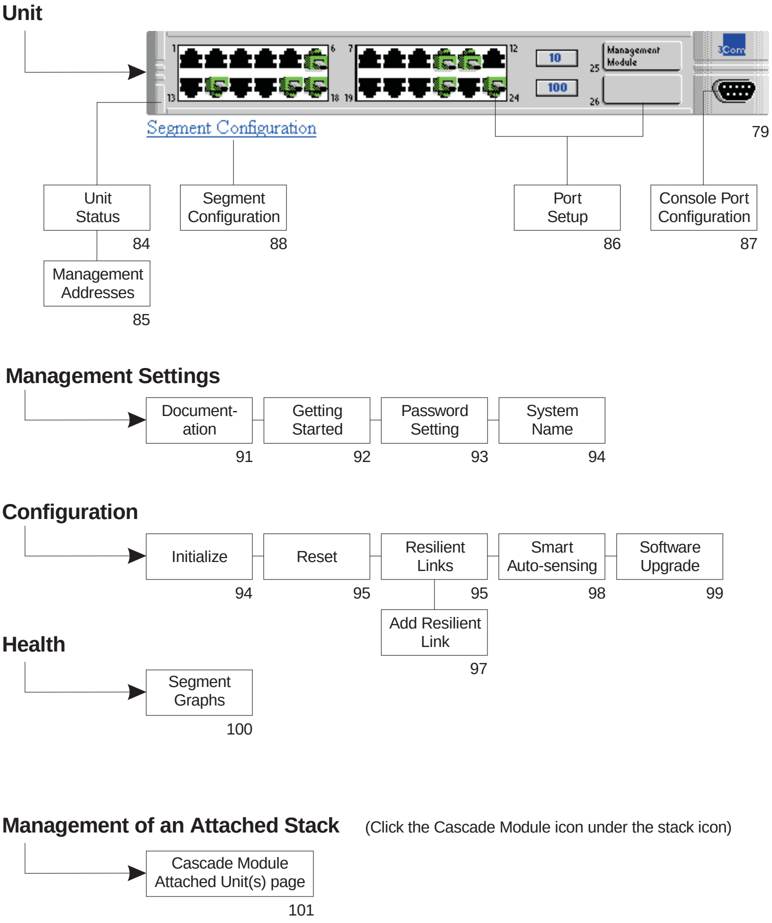
When you click on the management categories or stack icon, the page area changes to show various kinds of information. A page can consist of these components:

- **Fields** — Display current values and allow you to enter new values if required.
- **Checkboxes** — Show whether options are enabled (checked) or disabled (unchecked). Click on the checkboxes to change them.
- **Action buttons** — Affect the information in the fields and checkboxes for that page.
- **Page links** — Link to other pages of information within the same management category.

Web Interface Map

Figure 10 shows how the pages in the web interface are linked. The page number under each box is where the description is in this chapter.

Figure 10 Web Interface Map

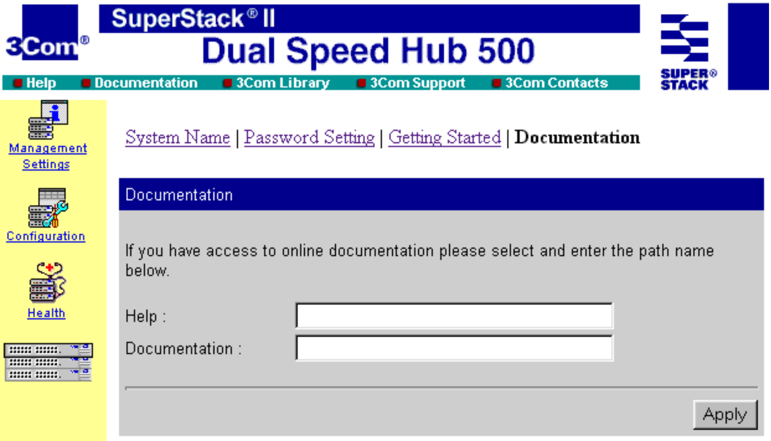


Using the Web Interface

To display management category pages:

1 Click on the management category (on the side bar) that you require. The page area changes to show a row of page links and the first page in that category, as shown in Figure 11. You can make changes to the information on the current page and click *Apply* when finished.

Figure 11 A Management Category Page



System Name | Password Setting | Getting Started | **Documentation**

Documentation

If you have access to online documentation please select and enter the path name below.

Help :

Documentation :

2 To display another page in that management category, click on the link in the row of links. The page area changes to show the new page.

3 Make changes to the information on the page as necessary (click *Apply* when finished) and choose another when ready. When you have finished, simply choose another management category from the side bar.

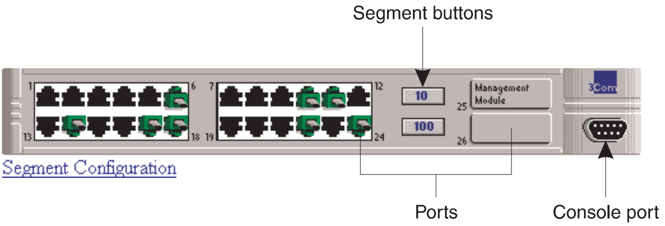
Unit View and Unit Pages

To display the Unit View and the Unit pages:

1 Click on the unit in the stack icon. The page area changes to show the Unit View and the Unit Status page. You can make changes to the information on the current page and click *Apply* when finished.

2 To display another page, click on part of the Unit View or the links underneath it, as shown in Figure 12.

Figure 12 Areas of the Unit View



If you click on:

- The unit (but not on a port or button) — The Unit Status page is redisplayed.
- A 10BASE-T or transceiver module port — The Port Setup page is displayed for that port.
- The console port — The Console Port Configuration page is displayed.
- A segment button — The Unit View is redisplayed indicating the ports that are connected to that segment.
- The *Segment Configuration* link — The Segment Configuration page is displayed.

3 You can make changes to the information on the page (click *Apply* when finished) and choose another when ready. When you have finished, simply choose another management category from the side bar.

For more information on the Unit View, refer to "Unit View" on page 83.

User Access Levels

For information on what the different user levels can manage, refer to "Default User Names and Passwords" on page 38.

Exiting the Web Interface

You can exit from the web interface at any time by closing your Web browser.

Online Help System and Documentation

The CD-ROM supplied with the management module has an online help system and online documentation which can be used with the web interface:

- The online help system is in Web format (HTML) so when it is launched, it appears in your Web browser.
- The online documentation is an online version of this user guide in Web format (HTML).

To use the online help system and user guide:

1. Decide how you want the web interface to access the files. You can either:
   - Copy the files onto your management station's local drive or place the CD-ROM in your management station's CD-ROM drive.
   - Copy the files onto a network drive or place the CD-ROM in a network CD-ROM server.
   - Copy the files onto a Web server.
2. Copy **all** of the files into a chosen directory (if required). On the CD-ROM, the files are in these directories:
   - Help system — **`Agent\`***version***`\Help`**
   - Documentation — **`Agent\`***version***`\Docs`**

   When copying the files, ensure that all the filenames are copied in lowercase letters. If copying to a UNIX system, there may be an option on your File Transfer program that will do this for you.
3. In the Documentation page (in the Management Settings category), specify the location of the online files. For information on how to do this, refer to "Documentation" on page 91.

The web interface always tries to point to the address you give it. If you have the online files on your management station's local drive, when other users try to access the files, the web interface will try to point to your files on their management stations, which may or may not exist. For this reason, it is a good idea to use a network drive or network CD-ROM server that is accessible to everyone who is going to use the web interface, so that the files are always in the same drive and directory for all users.

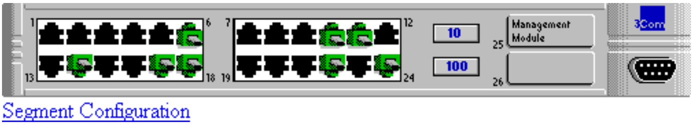
Unit Pages

This section describes the fields that appear on the pages in the Unit category. The first page displayed is the Unit Status page (together with the Unit View).

Unit View

The Unit View is a graphical version of the unit, as shown in Figure 13.

Figure 13 Unit View



To refresh the Unit View (to show any new changes), click *Refresh*. If the Unit View fails to show the latest port changes after a refresh, you must make a small configuration change to your Web browser; refer to "Configuring Your Browser" on page 36.

Port Status

The TP ports and transceiver module ports (if modules are fitted) are color coded to show their condition. To display this information in the web interface, click *Color Key*:

- **Black** — The port is enabled and has no connection.
- **Green** — The port is enabled and has a connection.
- **Gray** — The port has been disabled by management.
- **Red** — The port has partitioned (disabled itself). This may be due to:
  - *A network loop* — This occurs when there are too many active paths around the network.
  - *Receive jabber* — This occurs when the transmitting device is sending continuous data.
  - *False carrier events* — This occurs when poor quality cabling is used for 100Mbps.
- **TP connector with a red cable** — The connection has been changed from 100Mbps to 10Mbps by Smart auto-sensing. This may be due to poor quality cabling.

Identifying Which Ports Belong to a Segment

To view which ports belong to a segment, click on the 10Mbps or 100Mbps segment buttons on the Unit View. The graphic changes and ports that are members of that segment are highlighted with a dark blue surround.

Unit Status

This page provides detailed information about the unit:

System Name The name configured for the stack.

Location Where the stack is located.

Contact The person to contact if there is a problem with the stack.

The System Name can be configured using the System Name page (in the Management Settings category), refer to "System Name" on page 94. The Location and Contact can be configured using an SNMP network management application.

Unit Description The unit's product name.

Hardware Rev The version of hardware inside the unit.

MAC Address The unit's MAC (Ethernet) address.

Software Version The version of management software that the unit is running.

Boot PROM Version The version of software on the Boot PROM inside the unit.

Product Number Displays the 3Com product number of the unit.

TFTP Server (optionally displayed) Displays the IP address of the last TFTP server used to upgrade the unit's management software.

Filename (optionally displayed) Displays the name of the management software file that was used during the last software upgrade attempt.

Software Upgrade Status (optionally displayed) Displays the reason for a software upgrade failure.

Unit Uptime The time that has elapsed since the unit was last reset, initialized or powered on.

Unit Attention Light Causes the unit's Mgmt/Attn LED to flash. You can use this LED to help identify the unit in the stack.

To display the Management Addresses page, click *IP Setup* at the bottom of the Unit Status page.

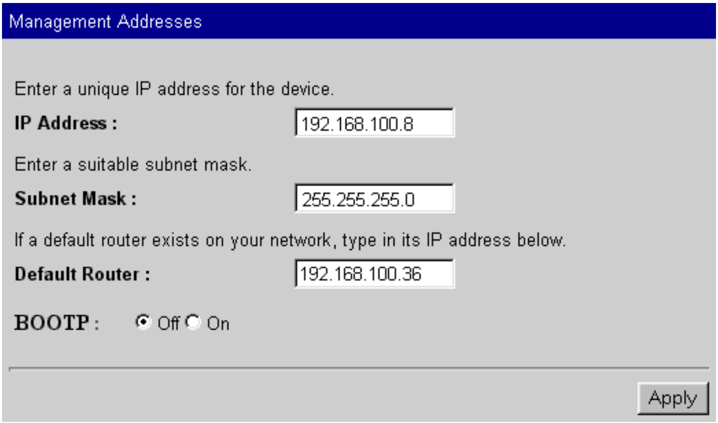
Management Address

This page specifies a unique IP address for the unit (which can be used to access the stack over the network), as shown in Figure 14.

If you have no previous knowledge of IP, refer to "IP Addresses" on page 30. If you change any of these values, you may need to re-access the stack using the new values.

Any changes that you make will take effect after a few seconds. You do not need to reset the stack.

Figure 14 Management Address Page



Management Addresses

Enter a unique IP address for the device.

IP Address : 192.168.100.8

Enter a suitable subnet mask.

Subnet Mask : 255.255.255.0

If a default router exists on your network, type in its IP address below.

Default Router : 192.168.100.36

BOOTP : ● Off ○ On

The fields are:

IP Address Provides a box for you to type the IP address of the stack.

Subnet Mask Provides a box for you to type the subnet mask for the IP address.

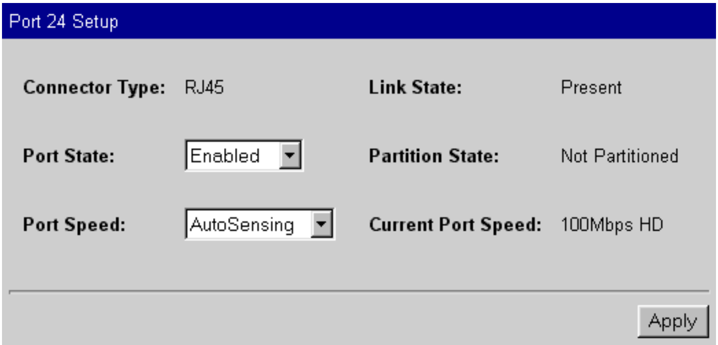
Default Router Provides a box for you to type the IP address of the default router (if you have one) which is used by the stack to communicate with other networks.

BOOTP Off / On
Specifies whether you want your BOOTP server (if you have one) to automatically allocate the stack an IP address and subnet mask.

Port Setup

This page specifies the port state (enable or disable), port speed, link state and partition state of the port, as shown in Figure 15.

Figure 15 Port Setup Page



Port 24 Setup

Connector Type:	RJ45	**Link State:**	Present
Port State:	Enabled	**Partition State:**	Not Partitioned
Port Speed:	AutoSensing	**Current Port Speed:**	100Mbps HD

The fields are:

Connector Type Shows the type of cable connector used to connect to the port.

Link State Shows the state of the port. This can be 'Present' or 'Not present'. If this field is blank, the cable connected to the port does not transmit a link state.

Port State Enabled / Disabled
Specifies whether the port can repeat information to and from the network.

If the port is part of a resilient link, you cannot enable or disable the port. You must first delete the resilient link. For more information on resilient links, refer to "What are Resilient Links?" on page 96.

Partition State Shows whether the port is capable of repeating traffic, or has automatically partitioned (isolated itself). If the port has partitioned, it may be due to a network loop, receive jabber or false carrier events (on 100Mbps).

Port Speed AutoSensing / 10Mbps HD / 100Mbps HD
Specifies the speed of the port. Different options are available depending on the port type (or what is connected to the port). By default, the ports on the front of the unit are set to auto-sensing

(auto-negotiation). We recommend that you keep this setting so that you have maximum flexibility when connecting devices to the unit.

The front panel ports on the Dual Speed Hub 500 and any transceiver modules (that are used in the transceiver module slots) can only operate in half duplex mode (shown by 'HD').

The Distance Extender Module is a 100Mbps transceiver module that you can use with the Dual Speed Hub 500. The 100BASE-TX module can only operate in half duplex mode, and the 100BASE-FX module can operate in either full duplex mode or half duplex mode (this is selectable by using the switch on the module). Refer to the documentation that accompanies the module for information on how to use it.

There are two levels of auto-sensing: 10/100 auto-sensing and Smart auto-sensing. By default Smart auto-sensing is enabled for the stack. It extends the normal auto-sensing functionality by monitoring any 100Mbps connections and, if necessary, downgrading them to 10Mbps connections if they are unsuitable at 100Mbps and will operate better at 10Mbps.

If you set a port to a specific speed and then try to use the port with equipment that operates at a different speed, the port will isolate itself and the Port Status LED for that port may flash on the unit. Smart auto-sensing will not affect ports that have been fixed to a specific speed (either 10Mbps or 100Mbps) using the Port Speed field.

Current Port Speed Shows the current port speed and duplex mode ('HD' is half duplex, 'FD' is full duplex).

If the connection has been downgraded from 100Mbps to 10Mbps by Smart auto-sensing (probably due to poor quality cabling), there is a line of red text under the Current Port Speed field informing you of this change. For information on configuring Smart auto-sensing, refer to "Smart Auto-sensing" on page 98.

Console Port Configuration

This page configures the console port.

The console port on the Dual Speed Hub 500 is already correctly configured by default, for direct connection to a management station. Only alter these default settings if you are connecting a modem to the console port.

***CAUTION:** Do not change any of these settings unless you fully understand what you are doing. Incorrect settings may lock you out from the unit's console port, and you may have to contact your supplier for information on recovering management communication if you cannot access the unit over the network.*

If you want to change the settings but are unsure of the correct settings to use, refer to the user documentation that accompanies your terminal or modem.

The fields are:

Console connection Terminal / Modem
Specifies what you are connecting directly to the console port. If you are connecting to a modem, select 'Modem', otherwise leave as 'Terminal' (management station).

Port Speed AutoConfig / 1200 / 2400 / 4800 / 9600 / 19,200
Specifies the baud rate of your management station or modem. The unit can automatically configure its baud rate to work with your management station or modem. Leave this field as 'AutoConfig' if you require auto-configuration.

Flow Control None / Hardware RTS/CTS
Specifies the flow control option that corresponds to your management station or modem.

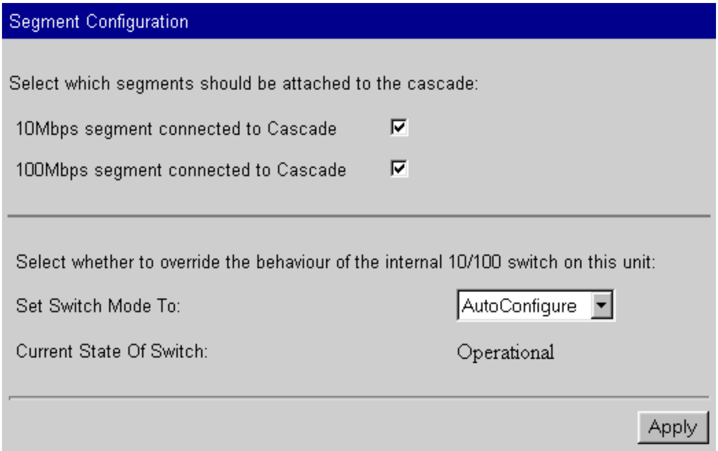
Segment Configuration

This page configures the segments (10Mbps and 100Mbps) and the segment switch for the unit, as shown in Figure 16.

When you connect 10Mbps and 100Mbps equipment to the unit, the ports are automatically connected to the relevant segment. The segment switch joins the 10Mbps and 100Mbps segments so that all of the equipment connected to the segments can communicate.

By default, the Dual Speed Hub 500 is configured so that all of its segments are connected, and its switch is in 'AutoConfigure' mode. This ensures that all equipment connected to the stack can communicate through the stack. Only alter the settings on this page if you want to alter the operation of the unit's switch.

Figure 16 Segment Configuration



Segment Configuration

Select which segments should be attached to the cascade:

10Mbps segment connected to Cascade ☑

100Mbps segment connected to Cascade ☑

Select whether to override the behaviour of the internal 10/100 switch on this unit:

Set Switch Mode To: AutoConfigure

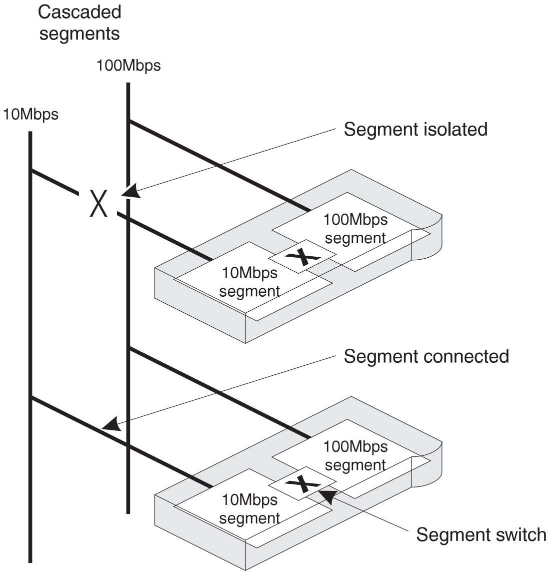
Current State Of Switch: Operational

The fields are:

10Mbps segment connected to Cascade Allows you to connect or isolate the 10Mbps segment from the 10Mbps cascaded segment that is connected to other units in the stack, as shown in Figure 17.

Isolating the segment (unchecking the checkbox) means that 10Mbps traffic received by the unit is not passed on to other units in the stack (unless it is passed on by the 100Mbps segment, if that segment is not isolated and the unit’s segment switch is operational).

Figure 17 Connected and Isolated 10Mbps Segments (Logical View)



100Mbps segment connected to Cascade Allows you to connect or isolate the 100Mbps segment from the 100Mbps cascaded segment that is connected to other units in the stack. Figure 17 shows an example of connected and isolated 10Mbps segments.

Isolating the segment (unchecking the checkbox) means that 100Mbps traffic received by the unit is not passed on to other units in the stack (unless it is passed on by the 10Mbps segment, if that segment is not isolated and the unit's segment switch is operational).

Set Switch Mode To AutoConfigure / Off
Specifies whether you want the unit's internal switch to be automatically configured by the stack or disabled. If set to 'AutoConfigure', the switch may be active or inactive depending on the configuration of other units in the stack.

There can only be one active switch linked to the stack's cascaded segments, in order to avoid a network loop.

Current State Of Switch Displays the mode of operation for the unit's internal switch. The switch can be:

- *Operational* — The switch is active and passing traffic between the 10Mbps and 100Mbps segments in the unit.
- *Standby* — The switch is inactive but will become active if required by the stack (and if the unit is the bottom unit in the stack). This may happen if the currently active switch is disabled or disconnected from one or both of the stack's cascaded segments.
- *Off* — The switch is disabled.

CAUTION: *The Hub's management facilities are accessed internally via the 10Mbps segment. If you try to disable the segment switch on the bottom unit of the stack over a 100Mbps connection (via the command line interface or the web management interface), you will lose the management connection. If this should occur, follow the procedure given on page 65, "Management Recovery Procedure".*

*If you have a Dual Speed Hub 500 with a serial number less than **0600/00000000000**, upgrading the software to version 2.1x or above will not give you support for segment configuration.*

Management Settings Pages

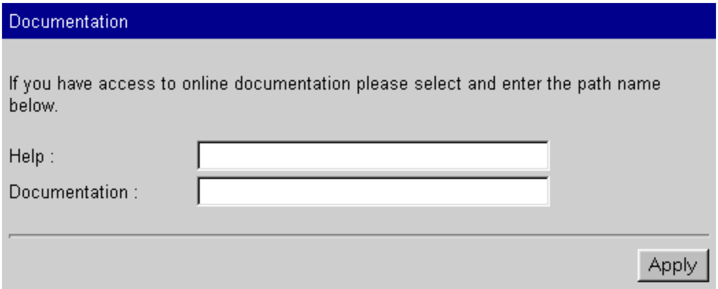
This section describes the fields that appear on the pages in the Management Settings category. The first page displayed is the Documentation page.

Documentation

This page specifies the directories or URLs that are used to access the online help system and documentation, as shown in Figure 18.

To access to online help system and documentation, the files must be set up; refer to "Online Help System and Documentation" on page 82. When specifying the locations of the files in the fields on this page, use forward-slashes (/) instead of back-slashes (\). For example, `c:\myfile` *becomes* `c:/myfile`*.*

Figure 18 Documentation Page



Documentation

If you have access to online documentation please select and enter the path name below.

Help :

Documentation :

The fields are:

Help Specifies where the online help system can be found. Enter the appropriate directory or Web address. Examples are:

- **`file://f:/help/index.htm`**
- **`http://yournetwork.com/help/index.htm`**

Documentation Specifies where the online documentation can be found. Enter the appropriate directory or Web address. Examples are:

- **`file://f:/documentation/index.htm`**
- **`http://yournetwork.com/docs/index.htm`**

The locations specified for the help system and documentation must both have **`index.htm`** *on the end.*

Getting Started

The Getting Started pages are a series of pages which set up basic information for the stack. You are asked:

- For a descriptive name for the stack.
- If you want to allocate the stack IP information or leave the allocation to a BOOTP server on your network (if you have one). A BOOTP server automatically allocates IP addresses to all equipment on your network.

  If you chose to allocate the IP information, you are asked:

  - For an IP address and subnet mask for the selected unit.
  - For an IP address for a default router — You may have a default router which you want the unit to use to communicate with other networks.

- The file path or Web address (URL) for the online help system and documentation files.
- To enter a new password (you can leave it blank if you don't want to change it).

If you have no previous knowledge of IP, refer to "IP Addresses" on page 30.

You do not need to use the Getting Started pages to configure this information, as it can all be configured using other pages in the web interface.

If you have already configured some of this information for the stack, it appears in the appropriate fields on the pages.

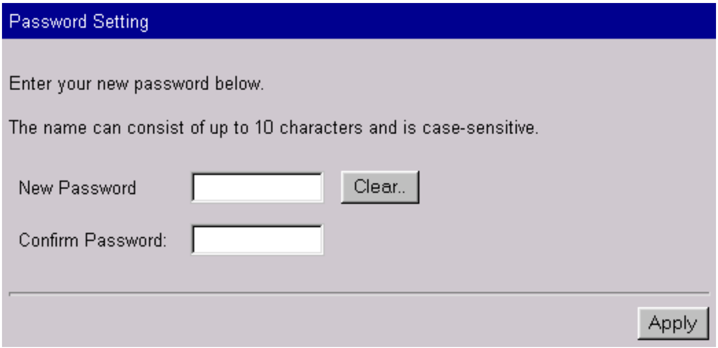
When you have entered the information in a page, click *Apply* to display the next page. You can use the back button of your Web browser to return to a previous page. When you display the last page, click *Finish* to accept the changes you have made and to exit from the Getting Started pages.

If you have changed any of the IP information, you may need to re-access the web interface using the new IP address.

Password Setting

This page changes the password for the user level that you are using, as shown in Figure 19. The passwords that you type do not appear on the screen.

Figure 19 Password Setting Page



Password Setting

Enter your new password below.

The name can consist of up to 10 characters and is case-sensitive.

New Password

Confirm Password:

The fields are:

New Password Type the new password you want to use.

Confirm Password Retype the password for confirmation.

Clear Button Clears the *New Password* and *Confirm Password* fields so that you can retype your new password if you make a mistake when typing into those fields.

If you change the password, a message appears informing you that the Web browser can no longer access the stack (this is because the Web browser is still using the old password). If you click OK to accept the message, the password panel appears so you can enter the new password to re-access the stack.

System Name

This page allows you to enter a name for the stack. Use a descriptive name, for example 'First floor stack'.

The name that you specify for the stack appears on some of the command line interface and web interface pages.

Configuration Pages

This section describes the fields that appear on the pages in the Configuration category. The first page displayed is the Initialize page.

Initialize

This page is used to initialize the stack. Initializing the stack causes it to return to its factory default settings, and the stack is reset. You may want to do this if the stack has been previously used in a different part of your network, and its settings are incorrect for its new environment.

CAUTION: *Initializing the stack removes all configuration information including resilient links and passwords (you will need to use the default password to re-access the stack). However, IP, SLIP and default router information is retained to ensure you can continue management communication with the stack over the network.*
If you have any resilient link set up for the stack, you may experience network loops after the initialize.

During an initialize, the Web browser is unable to communicate with the stack. After the initialize, communication is restored. The initialize process takes about 10 seconds.

Reset

This page is used to reset the stack. Resetting the stack simulates powering on and powering off the stack. You may want to do this if you want to reset the stack's statistics counters.

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

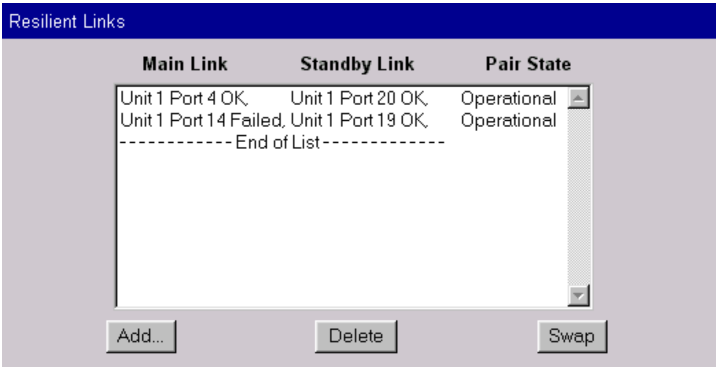
During a reset, the Web browser is unable to communicate with the stack. After the reset, communication is restored. The reset process takes about 10 seconds.

Resilient Links

This page shows the resilient links that have been set up for the stack, as shown in Figure 20.

Only media that generates a link pulse (for example twisted pair and fiber optic) can be part of a resilient link. This means that you can use the TP ports on the front of the Dual Speed Hub 500 and the transceiver module ports on the rear (if fitted with modules that have the required media).

Figure 20 Resilient Links Page



Resilient Links

Main Link	Standby Link	Pair State
Unit 1 Port 4 OK,	Unit 1 Port 20 OK,	Operational
Unit 1 Port 14 Failed,	Unit 1 Port 19 OK,	Operational

------------End of List-------------

The fields are:

Main Link Shows the unit and port number of the main link, and the state of the link.

Standby Link Shows the unit and port number of the standby link, and the state of the link.

Pair State Shows whether the resilient link pair is operational or not. When operational either the main port or the standby port can repeat traffic.

Adding, Deleting and Swapping Links

To add a resilient link pair to the list, click *Add*. The Add Resilient Link page is displayed.

To delete a resilient link pair from the list, click on the entry in the list and then click *Delete*. The resilient link pair is deleted, and the current active link remains enabled and the standby link is cancelled.

To swap the main and standby ports for a resilient link pair in the list, click on the entry in the list and then click *Swap*.

What are Resilient Links?

You can make the network more robust by adding *resilience* to it. When a link fails all communication between equipment on each side of the link is lost. To ensure important communication is not lost, the network needs to be reinstated immediately which could be very inconvenient for the network manager. If a spare link was configured to automatically pick up when the broken link failed, the network would appear to function normally to the user. At worst, a few packets would be corrupted or lost.

This is the concept of resilient links. One link is on standby (called the *standby* link) waiting to take over if another link (called the *main* link) fails. This pair is called a *resilient link pair*. The resilient link ports can be on different units in the stack, and any network devices can be at the other ends of the links.

When the network is in use, the stack that has been used to set up the resilient link pair, monitors the state of both the main link and the standby link. If the main link fails, the standby link becomes active.

You can use the Resilient Links page to view the status of the links. If you have an SNMP network management application, you can configure the unit to send *traps* (messages) to the SNMP network management application, if the states of the links change.

Resilient Link Pairs

To set up a resilient link pair, you need to manage the stack that both links in the pair are connected to. The number of resilient link pairs you can set up is only restricted by the number of ports you have in the stack.

When you set up the resilient link pair, you need to specify the ports that the main link and standby link are connected to.

Resilient Link Rules

Always follow these rules when setting up a resilient link pair:

- Only media that generates a link pulse (for example 10BASE-T, 100BASE-TX, 100BASE-FX and fiber optic) can be part of a resilient link. This means that you can use the TP ports on the front of the Dual Speed Hub 500 and the transceiver module ports on the rear (if fitted with modules that have the required media).
- Configure the resilient link pair at only one end of the link. In other words, only one stack controls each resilient link pair you set up.
- Each resilient link pair can only have one main link and one standby link (the ports used can be on different units in the stack).
- Each link must not belong to more than one resilient link pair.
- Do not enable security for ports that are part of a resilient link pair.

If the main link fails, the standby link becomes active.

Add Resilient Link

This page is used for adding resilient links to the stack. Choose the main link and click *Next*, and then choose the standby link and click *Next*. The resilient link pair appear in the list on the Resilient Links page.

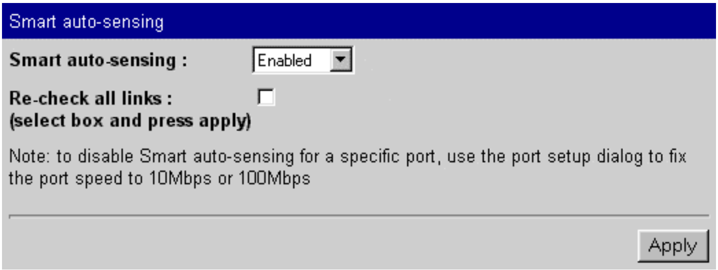
Smart Auto-sensing

You can use the Smart Auto-sensing page to configure Smart auto-sensing for the stack, as shown in Figure 21. By default, Smart auto-sensing is enabled for the stack.

Smart auto-sensing checks the quality of any new 100Mbps connection made to the stack. If the connection is unsuitable, it automatically downgrades the connection to 10Mbps. For more information on Smart auto-sensing, refer to "Smart Auto-sensing Feature" on page 16.

Smart auto-sensing does not affect ports that are fixed to a specific speed (10Mbps or 100Mbps). To fix a port to a specific speed, use the Port Speed field on the Port Setup page. Refer to "Port Setup" on page 86.

Figure 21 Smart Auto-sensing Page



Smart auto-sensing

Smart auto-sensing : Enabled

Re-check all links : □
(select box and press apply)

Note: to disable Smart auto-sensing for a specific port, use the port setup dialog to fix the port speed to 10Mbps or 100Mbps

The fields are:

Smart auto-sensing Enabled / Disabled
Specify whether you want Smart auto-sensing enabled or disabled for the stack.

Recheck all links If Smart auto-sensing is enabled for the stack, this checkbox is displayed allowing you to prompt the Smart auto-sensing feature to recheck all connections. Note that Smart auto-sensing automatically rechecks all new cable connections. Rechecking all links is useful to do if abnormal conditions have caused network errors (such as electrical interference near to the network). To recheck all connections, select this checkbox and click *Apply*.

Software Upgrade

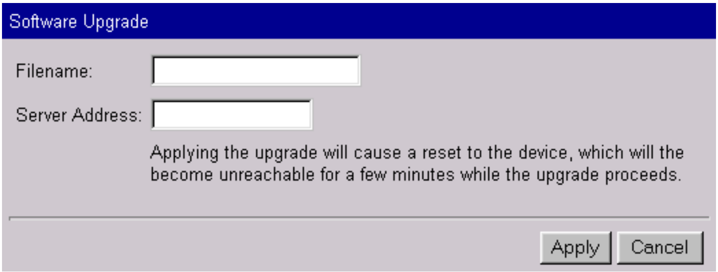
When 3Com issues a new version of the management software agent for the Dual Speed Hub 500, you can upgrade the units in your stack. This page is used to upgrade the stack, as shown in Figure 22.

You must copy the new management software agent into the appropriate directory on a TFTP server (use the directory that the TFTP server has been configured to look in). For information on how to use your TFTP server, refer to the documentation that accompanies it.

During a software upgrade, the Web browser is unable to communicate with the stack. After a successful upgrade, the stack resets itself and communication is restored. The upgrade process may take up to 5 minutes for each unit.

When you upgrade a stack, the new management software is stored in each unit. If you add a unit that is running a different version of management software, you must upgrade the unit to ensure that all of the units have the same functionality.

Figure 22 Software Upgrade Page



Software Upgrade

Filename:

Server Address:

Applying the upgrade will cause a reset to the device, which will the become unreachable for a few minutes while the upgrade proceeds.

The fields are:

Filename Type the file name of the upgrade file. The file name format is **`DSH`***xx_yy***`.bin`**, where *xx_yy* is the version of agent software, for example **`DSH02_00.bin`**.

Server Address Enter the IP address of the TFTP server that has the software upgrade on it.

A power interrupt during the software upgrade may cause a corrupted agent image on the hub. If this occurs then subsequent rebooting of the unit will be unsuccessful and the power LED will *flash. In this event the software should be updated using the "Serial Update Utility". See Appendix D on page 127 for details.*

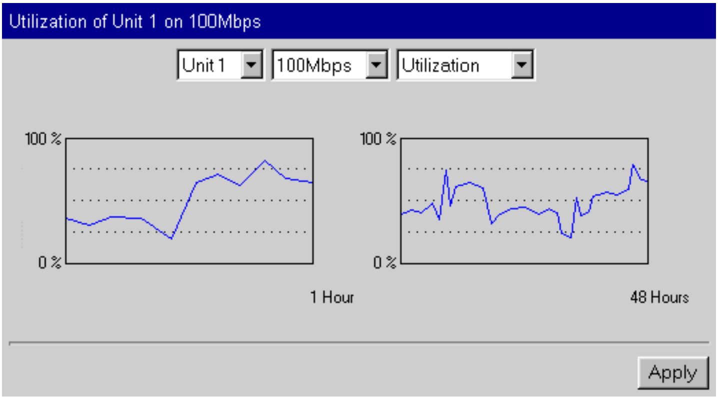
Health Pages

This section describes the fields that appear on the Segment Graphs page in the Health category.

Segment Graphs

This page shows two graphs for a unit in the stack. The first graph shows information for the last hour, the second graph shows information for the last 48 hours, as shown in Figure 23. These graphs are generated using JAVA.

Figure 23 Segment Graphs Page



Utilization of Unit 1 on 100Mbps

Unit 1 ▾ 100Mbps ▾ Utilization ▾

The fields are:

Unit Specifies the unit that has the segment.

Segment Specifies the segment that the graphs are displayed for.

Graph Type Specifies the type of graph that is displayed:

- *Utilization* — Shows the current amount of bandwidth that is used on the segment. A high bandwidth level could indicate high network activity, which can slow network response times.
- *Total Errors* — Shows the current total number of packets with errors that have been seen by the ports (for that segment) since the stack was last reset or initialized. A high number of errors

could indicate that there is faulty equipment somewhere on the network, or that the network is badly configured.

Accessing a Different Hub or Stack

If a different type of unit or stack is connected to the Dual Speed Hub 500 stack with a Cascade Converter Kit, you can access its management screens from the Dual Speed Hub 500 web interface.

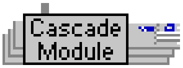
Management software agent version 1.20 (shipped with the Cascade Converter Kit) or later must be installed on the Dual Speed Hub 500. For information on upgrading, refer to "Software Upgrade" on page 99.

Using the Dual Speed Hub 500 – Hub 10 Cascade Converter Kit, you can connect a managed Hub 10 unit or stack to the Dual Speed Hub 500 stack. For more information, refer to "Management of a Different Hub or Stack" on page 17.

To access the management screens of the attached stack:

1 Click on the Cascade Module icon that is below the stack icon on the side bar of the web interface, as shown in Figure 24.

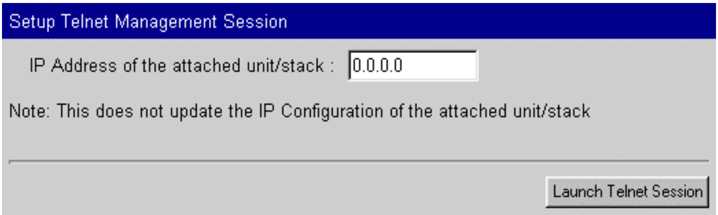
Figure 24 Cascade Module Icon



The Cascade Module icon does not reflect the number of units in the attached stack. When you connect the unit or stack to the Dual Speed Hub stack, it may take 30 seconds to register the connection. If the Cascade Module icon is not present, you may need to reload the web interface page at your Web browser.

The web interface changes to show the Cascade Module Attached Unit(s) page, as shown in Figure 25. The management categories on the side bar are inactive except for the stack icon, which returns you to the Dual Speed Hub 500 web interface when one of the units in the icon is clicked.

Figure 25 Cascade Module Attached Unit(s) Page



Setup Telnet Management Session

IP Address of the attached unit/stack : 0.0.0.0

Note: This does not update the IP Configuration of the attached unit/stack

2 In the IP Address field, specify the IP address of the attached stack (for example a Hub 10 stack) and click *Launch Telnet Session*. The specified IP address is remembered by the Dual Speed Hub 500 and is displayed in the IP Address field for future management sessions.

Remember that:

- If you enter an IP address of '0.0.0.0', you get an error.
- If you change the IP address of the attached stack, you must re-enter the new IP address in the Cascade Module Attached Unit(s) page when starting the next management session.
- If you enter the wrong IP address, the web interface fails to find the attached stack and may display the management screens for a different device on your network (that has the IP address you entered).

If your Web browser has been configured to start a Telnet application, the web interface starts the Telnet application and passes the IP address to it. When the attached stack is found, its management interface is displayed in the Telnet application, and you are now ready to manage the unit or stack. Refer to the documentation that accompanies the attached stack (or its management module) for information on using its management interface.

If your Web browser has not been configured to start a Telnet application, a message appears asking you to pick a suitable application to view the management interface. Browse for a Telnet application. To configure your Web browser to start a Telnet application for future management sessions, refer to "Configuring Your Browser" on page 103.

The attached stack's management session in the Telnet application is completely separate from the web interface, so you can:

- *Launch multiple Telnet sessions — this is restricted by the number of management sessions allowed by the attached stack's management.*
- *Continue to manage the Dual Speed Hub 500 stack while managing the attached stack.*

Configuring Your Browser

If you are accessing a Hub 10 stack's management screens through the Dual Speed Hub 500 stack's web interface, your Web browser must be configured to start a Telnet application.

To do this for Netscape Navigator:

1. In Netscape Navigator, from the *Options* menu, select *General Preferences*. The preferences dialog box appears.
2. Select the *Apps* tab.
3. In the Apps property sheet, specify the location and filename of the Telnet application (browse for it if required). For Windows 95, a suitable application is `telnet.exe` which may be found in the `Windows` directory on your hard drive.
4. Click *OK*.

5 PROBLEM SOLVING

The Dual Speed Hub 500 has been designed to aid you when detecting and solving possible problems with your network. These problems are rarely serious, the cause is usually a disconnected or damaged cable, or incorrect configuration.

This chapter has information on solving management problems, that involves the use of the management module. If the information given does not solve your problem, contact your supplier for information on what to do next. If you have a problem with the unit, refer to the user guide that accompanies the unit.

If you have a problem with the serial web utility, refer to "Solving Problems With the Serial Web Utility" *on* page 120.

Perform these actions first:

- Ensure that any equipment to be attached to the Dual Speed Hub 500 has the latest version of its driver software installed, especially any network interface card.
- Ensure all equipment is powered on.
- Power each unit off, wait about 5 seconds and then power them on so they perform a self test. The self test only takes a few seconds, during which the Power/Self Test LED flashes.

Isolating a Problem

A good way of isolating a problem is to see whether it occurs on a particular port only. This can be done by:

- Using a different port to see if the problem still exists.
- Using management to view how a port has been set up. In particular, see if the port is:
  - Partitioned due to a network loop, receive jabber or false carrier events (on 100Mbps)
  - Disabled by management
  - Part of a resilient link pair
  - Performing security
  - Operating at the correct speed (10Mbps or 100Mbps)

Solving Problems With the Command Line Interface

The terminal or terminal emulator cannot access the stack through the console port on one of the units. Check that:

- Your terminal or terminal emulator is correctly configured to operate as a standard terminal. If this doesn't work, try configuring it to operate as a VT100 terminal.
- You have performed the wake-up procedure correctly, by pressing Return twice.
- Check the settings on your terminal or emulator. The parity must be set to 'none', the stop bit '1' and the data bits (character size) '8'. The management facility's auto-configuration works only with speeds 1200, 2400, 4800, 9600 and 19,200.
- You are using the right cable. For examples of the pin wiring for suitable cables, refer to "Console Cable" on page 113.

If you still cannot access the stack, reset the stack using the web interface and retry the wake-up procedure. If this does not work, initialize the stack.

The Telnet application cannot access the stack over the network. Check that:

- The stack's IP address, subnet mask and default router are correctly configured. Your Telnet application must point to the same IP address.

- The port through which you are trying to access the stack has not been disabled by another user (using the web interface or an SNMP network management application).
- You are using the right network cables. For examples of the pin wiring for suitable cables, refer to "10BASE-T and 100BASE-TX Cable" on page 111.

If your management station has a PING application, you can use it to try to access the stack to see if it can communicate with your management station. Check that you can access other devices. If you cannot access any other devices, there may be a problem with your Telnet application or management station.

If you still cannot access the stack, reset the stack using the web interface and try to re-access the command line interface. If this does not work, initialize the stack.

Initial password prompt is not displayed after a logout. Some Telnet applications require you to reconnect to the stack.

You forget your password. If you can access the stack using the security or admin user level, you can initialize the stack to reset the passwords. If you have forgotten all of your passwords, you must contact your supplier.

Solving Problems With the Web Interface

The Web browser cannot access the stack through the console port. Check that:

- If you have a management station running Windows® 95, you are using the 3Com serial web utility (SLIP Driver). Refer to Appendix B.
- You are using the correct SLIP address and SLIP subnet mask. The default SLIP address is '192.168.101.1', and the default SLIP subnet mask is '255.255.255.0'.
- You are using the right cable. For examples of the pin wiring for suitable cables, refer to "Console Cable" on page 113.

The Web browser cannot access the stack over the network. Connect to the stack's console port and use the command line interface to check that:

- The stack's IP address, subnet mask and default router are correctly configured; refer to "Displaying the IP Information" on page 52.
- The port through which you are trying to access the stack has not been disabled.
- You are using the right network cables. For examples of the pin wiring for suitable cables, refer to "10BASE-T and 100BASE-TX Cable" on page 111.

If your management station has a PING application, you can use it to try to access the stack to see if it can communicate with your management station.

The Web browser can no longer access the stack over the network. Check that the port through which you are trying to access the stack has not been disabled. If it is enabled, check the connections and network cabling at the port. Try accessing the stack through a different port. If you can now access the stack, a problem with the original port is indicated. Re-examine the connections and cabling.

Possibly there is a network problem preventing you from accessing the stack over the network. Try accessing the stack through its console port and reset the stack.

The Web browser cannot access the stack over a serial link from a Windows 95 management station. You must use the 3Com serial web utility (SLIP Driver). Check that it is installed correctly. Refer to "Installing the Serial Web Utility" on page 117.

Some of the web interface is not displayed in the Web browser after downloading. This is probably due to large amounts of traffic over the network. Either reload (download) the web interface, or click in the part of the web interface that has not displayed and select the reload frame option in your Web browser.

The Unit View does not display the latest port states. Every time you want to change the port states or want to update the Unit View, simply click *Refresh* (underneath the Unit View). If the Unit View fails to show the latest port changes after a refresh, you must make a small configuration change to your Web browser; refer to "Configuring Your Browser" on page 36.

The Unit View shows a TP connector with a red cable. This particular 100Mbps connection has been downgraded to a 10Mbps connection by the Smart auto-sensing feature (indicated by the red cable), as it a poor quality connection and performs better at 10Mbps. The reason for the poor quality may be the use of incorrect or damaged cables (Category 5 twisted-pair is required for Fast Ethernet), or that the connection travels through many patch panels before reaching the attached device.

The error message 'Incorrect user access level' is displayed on the web interface page. You are trying to perform a management operation that is not permitted for your user level.

The Cascade Module icon is not shown on the side bar, when a different unit or stack is connected with a Cascade Converter Kit. When you make the connection to the Dual Speed Hub stack, it may take 30 seconds to register the connection. If the Cascade Module icon is not present, you may need to reload the web interface page on your Web browser, or (if this does not work) close the Web browser and reconnect to the web interface. If the Cascade Module icon is still not shown, the Cascade Module may be fitted incorrectly.

Cannot access an attached unit or stack with the Cascade Module Attached Unit(s) page. Ensure that the IP address specified in the IP Address field matches the IP address of the attached unit or stack. The management module within the attached unit or stack may be fitted incorrectly.

After changing the password, the Web browser displays a message informing you that it can no longer access the stack. This is because the Web browser is still using the old password. If you click *OK* to accept the message, the password panel appears so you can enter the new password to re-access the stack.

You forget your password. If you can access the stack using the security or admin user level, you can initialize the stack to reset the passwords. If you have forgotten all of your passwords, you must contact your supplier.

Solving Problems With an SNMP Network Management Application

The SNMP network management application cannot access the stack. Check that:

- The stack's IP address, subnet mask and default router are correctly configured, using either:
  - The command line interface — refer to "Displaying the IP Information" on page 52.
  - The web interface — refer to "Management Address" on page 85.
- The stack's IP address is correctly recorded by the management application. For information on how to do this, refer to the documentation that accompanies the application.
- You can access other devices. If you cannot access any other devices, there may be a problem with your SNMP network management application or management station.

The SNMP network management application can no longer access the stack. Check that the port through which you are trying to access the stack has not been disabled. If it is enabled, check the connections and network cabling at the port. Try accessing the stack through a different port. If you can now access the stack, a problem with the original port is indicated. Re-examine the connections and cabling.

Possibly there is a network problem preventing you from accessing the stack over the network. Try accessing the stack through the console port of one of the hubs, and reset the stack.

A

Cabling and Management Settings

Management Settings

Table 9 shows the settings you need to set your management station's serial port to, if you are managing the Dual Speed Hub 500 directly through its console port.

Table 9 Management Station Settings

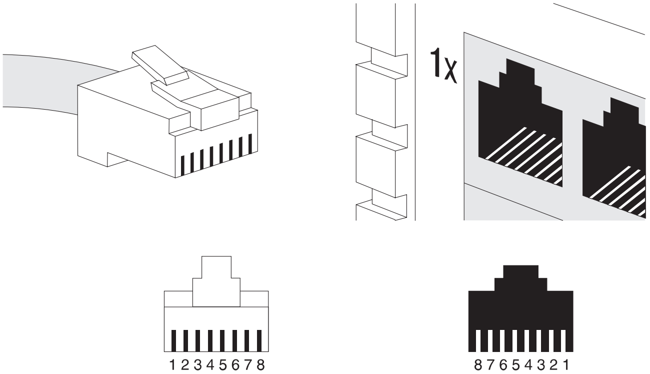
Data bits (character size)	8
Stop bit	1
Parity	None

Cabling

This section shows the pin-outs for the various cables that are used with the Dual Speed Hub 500. These cables are available from your supplier.

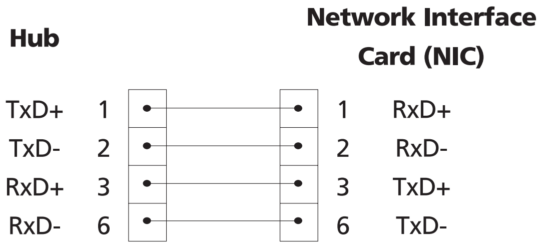
10BASE-T and 100BASE-TX Cable

Figure 26 Pin Numbering for 10BASE-T and 100BASE-TX



Straight-through

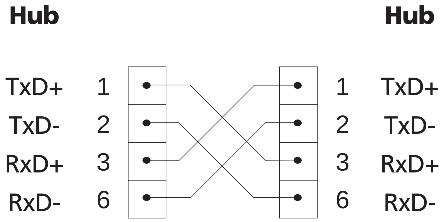
Figure 27 Straight-through 10BASE-T and 100BASE-TX Cabling



Pins 4, 5, 7 and 8 are not used

Crossover

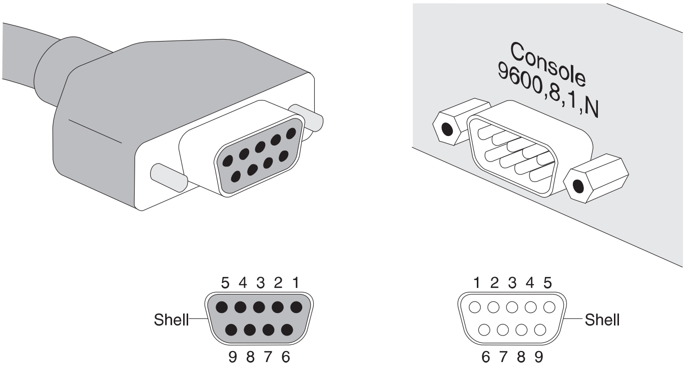
Figure 28 Crossover 10BASE-T and 100BASE-TX Cabling



Pins 4, 5, 7 and 8 are not used

Console Cable

Figure 29 Pin Numbering for Console



Examples of Null Modem Cables You Can Use

Figure 30 Example of Null Modem Cabling for 9-pin Management Station

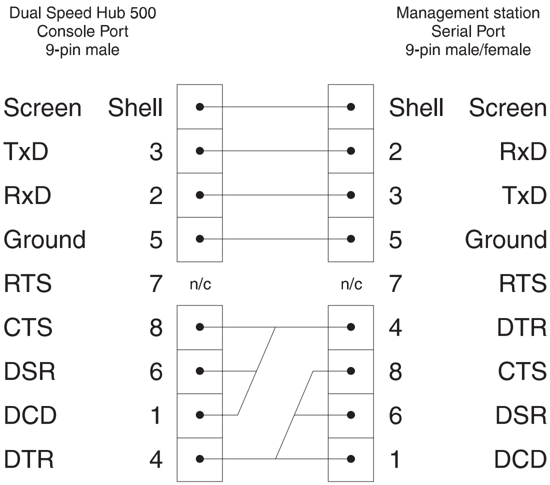
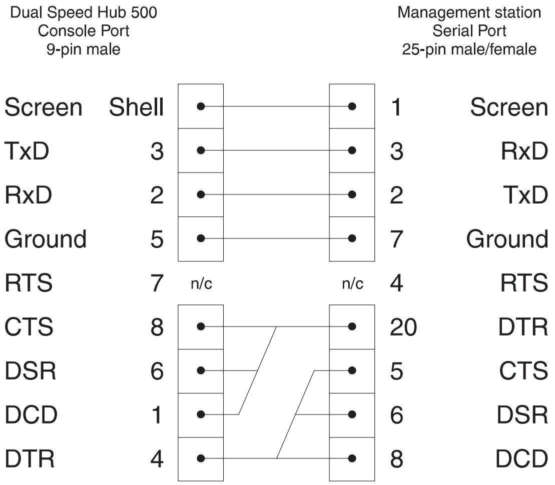
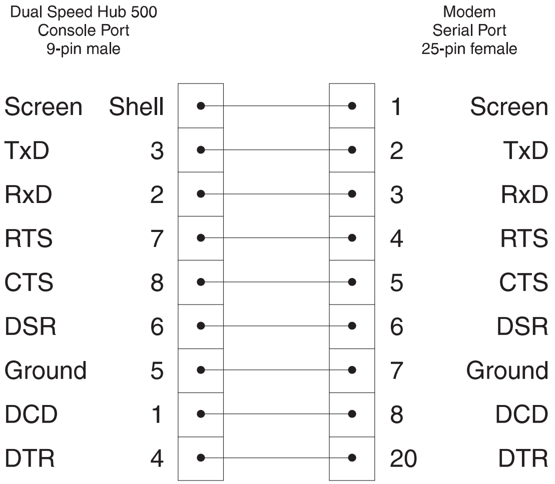


Figure 31 Example of Null Modem Cabling for 25-pin Management Station



Modem Cable

Figure 32 Example of Modem Cabling for 25-pin Management Station



Cascade Connections

Cascade cables are available in a range of lengths from your supplier. There are also Hot Swap Cascade Units which increase the resilience of your cascade connections, and Converters which enable you to connect PS Hubs and a Hub 10 stack to your Dual Speed Hub 500 stack. Table 10 shows the product numbers for these items. Contact your supplier for information about any other equipment that can be used with the Dual Speed Hub 500.

Table 10 Cascade Cables and Units

Number	Product
3C16695	0.3m (11.8in.) Cascade cable
3C16690	Hot Swap Cascade Unit
3C16686	Dual Speed Hub 500 – Hub 10 Cascade Converter Kit
3C16692	Dual Speed Hub – PS Hub Cascade Converter Kit

B SERIAL WEB UTILITY

Introduction

If you are using a management station running Microsoft Windows® 95 or 98 and want to access the web interface through the unit's console port, you must use the 3Com serial web utility (SLIP Driver) supplied on the CD-ROM that accompanies the management module.

*The 3Com serial web utility **only** works on Windows 95 or 98.*

Every time you want to access the web interface, use the serial web utility to set up the connection to the web interface; it launches your Web browser and accesses the web interface using SLIP for you.
If you have any problems accessing the web interface using the serial web utility, refer to "Solving Problems With the Serial Web Utility" on page 120.

Installing the Serial Web Utility

The serial web utility can be installed on to a management station that already has other 3Com management applications installed on it. The default directory into which the serial web utility is installed is `C:\Program Files\3Com\3Com Serial Web`. This can be changed during the installation if required.

The installation program is a standard Windows based installation. To install the serial web interface:

1 Start Windows.

If you already have an existing Transcend® management application running, ensure that it is closed down.

2 Insert the CD-ROM into your CD-ROM drive.

3 Select *Run* from the *Start* menu.

4 In the *Run* dialog box, type **`drive:\Win95\Drivers\Slip\SETUP`** (where *drive* is the letter of your CD-ROM drive) and click *OK*.

The installation program starts and checks your system configuration; enter any information that is requested.

If the setup program cannot find specific files on your management station, it asks you to insert your Windows CD-ROM. If it still cannot find the files, you must obtain them directly from Microsoft. Contact Microsoft for more information.

5 When the installation program has ensured all the relevant files are installed, it asks you to select the COM port. This is the serial port on your management station that you are going to use when connecting to the unit's console port.

If you click *Advanced*, the Advanced Configuration Parameters dialog box is displayed, showing all of the settings the serial web utility will use when it is run. These default settings are already correct for connection to the unit so you should not need to change them.

The fields are:

Connection name Allows you to enter a name for the connection.

Modem name Allows you to enter a name for the modem connection.

PC SLIP Address The SLIP address that is to be allocated to the management station. The default address is '192.168.101.2'.

Device URL The URL that the serial web utility uses to access the unit, which includes the unit's SLIP address. For example, the default SLIP address for the unit is '192.168.101.1' so the URL is:
`http://192.168.101.1/`

Flow Control None / XON/XOFF / Hardware RTS/CTS
Allows you to specify the flow control that the management station is to use.

Data bits, **Stop bits** and **Parity** are all fixed.

Speed 1200 / 2400 / 4800 / 9600 / 19,200
Allows you to specify the baud rate that the management station is to use.

You also have the option of changing the *PC SLIP Address*, *Device URL*, *Flow Control* and *Speed* after the installation is complete.

6 When you have finished, the final installation dialog box is displayed informing you that the serial web utility has been installed on your management station. Click on *Finish* to close the dialog box.

7 You are asked if you want to restart Windows so that it can use the new settings you have configured. You must restart Windows before running the serial web utility.

When you return to the Windows desktop, the serial web utility shortcut (‘Serial Web Management’) created by the installation program is visible. The utility also has its own program group called ‘Serial Web’ under the default program group specified during the install, which contains:

- *Serial Web Management* — Launches the serial web utility.
- *Serial Web Setup* — Displays the Advanced Configuration Parameters dialog box, which allows you to view and change some of the settings the serial web utility uses when it is run.
- *License agreement*.

Using the Serial Web Utility

Every time you want to access the web interface through a serial link, make your management connection (refer to “Through the Console Port” on page 35) and use the serial web utility to set up your connection:

1 Do one of the following:

- Double-click on the Serial Web Management shortcut.
- Select the Serial Web Management program item in the Serial Web program group.

2 The serial web utility opens and asks you if you want to use the URL that has been set up. The URL includes the unit’s SLIP address. For example, if the SLIP address for the unit is ‘192.168.101.1’, the URL is: **`http://192.168.101.1`**

If you want to change the URL, click *URL*. If the URL is correct, click *OK*.

3 The serial web utility attempts to establish a connection.

If successful, the standard Windows Dial-Up Networking dialog box is displayed, showing the various connection details. Your default Web browser is then launched with the specified URL.

4 The connection is successful if the web interface's password panel is displayed. You are now ready to manage the unit; refer to "Using the Web Interface".

Solving Problems With the Serial Web Utility

If you are unable to connect to the unit's web interface, it may be that:

- The unit is not powered on.
- You are not using a proper null modem cable, refer to "Examples of Null Modem Cables You Can Use" on page 113.
- The following settings are different on your unit and management station:
  - Flow control.
  - Speed (baud rate).
- The unit has automatically configured its communication speed, but you have subsequently changed the speed configured on your management station (the device only automatically configures the speed the first time it connects).
- You have selected the wrong COM port on your management station.

To change some of the settings for the management station, use the Advanced Configuration Parameters dialog box. To display this, select the Serial Web Setup program item in the Serial Web program group.

C

RMON

This appendix describes the concept of RMON and how it is implemented in the Dual Speed Hub 500. It contains the following topics:

- Overview of RMON and its benefits
- RMON features of the Dual Speed Hub 500

What is RMON?

Using the RMON (Remote Monitoring) capabilities of your Dual Speed Hub 500 allows network administrators to improve their efficiency and reduce the load on their network.

The following sections explain more about the RMON concept and the RMON features supported by the unit.

You can only use the RMON features of the unit if you have an RMON management application, such as the RMON application supplied with 3Com's Transcend® Enterprise Manager, or using a MIB browser.

RMON is the common abbreviation for the Remote Monitoring MIB (Management Information Base), a system defined by the IETF documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely. The Dual Speed Hub 500 supports RMON Version 1.

A typical RMON setup consists of two components:

- **The RMON probe** — an intelligent, remotely-controlled device or software agent that continually collects statistics about a LAN segment or VLAN, and transfers the information to a management workstation on request or when a pre-defined threshold is crossed.
- **The management workstation** — communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe and can manage the probe by in-band or out-of-band connections.

About the RMON Groups

The IETF define nine groups of Ethernet RMON statistics. This section describes these groups, and details how they can be used.

Statistics

The Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts and errors on a LAN segment.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of your network.

History

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.

The group is useful for analysis of traffic patterns and trends on a LAN segment, and to establish baseline information indicating normal operating parameters.

Alarms

The Alarms group provides a versatile, general mechanism for setting thresholds and sampling intervals to generate events on any counter or integer variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, the 3Com SmartAgent allows alarm thresholds to be autocalibrated.

Alarms are used to inform you of a network performance problem and they can trigger automated action responses through the Events group.

Hosts

The Hosts group specifies a table of traffic and error statistics for each host on a LAN segment. Statistics include packets sent and received, octets sent and received, as well as broadcasts, multicasts, and error packets sent.

The group supplies a simple discovery mechanism listing all hosts that have transmitted. The next group, Hosts Top N, requires implementation of the Hosts group.

Hosts Top N

The Hosts Top N group extends the Hosts table by providing sorted host statistics, such as the top 20 nodes sending packets or an ordered list of all nodes according to the errors they sent over the last 24 hours.

Matrix

The Matrix group shows the amount of traffic and number of errors between pairs of devices on a LAN segment. For each pair, the Matrix group maintains counters of the number of packets, number of octets, and error packets between the nodes.

The conversation matrix helps you to examine network statistics in more detail to discover who is talking to whom or if a particular PC is producing more errors when communicating with its file server, for example. Combined with Hosts Top N, this allows you to view the busiest hosts and their primary conversation partners.

Filter

The Filter group provides a mechanism to instruct the RMON probe to capture packets that match a specific criterion or condition.

Capture

The Capture group allows you to create capture buffers on the probe that can be requested and uploaded to the management station for decoding and presentation.

Events

The Events group provides you with the ability to create entries in an event log and/or send SNMP traps to the management workstation. Events can originate from a crossed threshold on any RMON variable. In addition to the standard five traps required by SNMP (link up, link down, warm start, cold start, and authentication failure), RMON adds two more: rising threshold and falling threshold.

Effective use of the Events group saves you time; rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions providing a mechanism for an automated response to certain occurrences.

Benefits of RMON

Using the RMON features of the Dual Speed Hub 500 has three main advantages:

- **It improves your efficiency**

  Using RMON probes allows you to remain at one management station and collect information from widely dispersed LAN segments. This means that the time taken to reach a problem site, set up equipment, and begin collecting information is largely eliminated.

- **It allows you to manage your network in a more proactive manner**

  If they are configured correctly, RMON probes deliver information before problems occur. This means that you can take action before they impact on users. In addition, probes record the behavior of your network, so that you can analyze the causes of problems.

- **It reduces the load on the network and the management station**

  Traditional network management involves a management station polling network devices at regular intervals to gather statistics and identify problems or trends. As network sizes and traffic levels grow, this approach places a strain on the management station and also generates large amounts of traffic.

  An RMON probe, however, autonomously looks at the network on behalf of the management workstation without affecting the characteristics and performance of the network. The probe reports by exception, which means that it only informs the management workstation when the network has entered an abnormal state.

RMON and the Dual Speed Hub 500

RMON requires one probe per LAN segment, and stand-alone RMON probes have traditionally been expensive. Therefore, 3Com's approach has been to build an inexpensive RMON probe into the SmartAgent® of each Dual Speed Hub 500. This allows RMON to be widely deployed around the network without costing more than traditional network management.

One other problem with stand-alone 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.

As an example, statistics can be related to the segments and the unit can take autonomous actions such as disabling a port on a segment (temporarily or permanently) if errors on that segment exceed a pre-defined threshold.

RMON Features of the Dual Speed Hub 500

All nine groups of RMON are supported fully for 10Mbps and 100Mbps segments.

*If you have a Dual Speed Hub 500 with a serial number less than **0600/00000000000**, upgrading the software to version 2.1x or above will not give you support for the RMON Filter and Capture groups on the 100Mbps segments, which means that you cannot perform RMON Filter Capture for the 100Mbps segments.*

Table 11 details the RMON support provided by the unit.

Table 11 RMON Support Provided by the Unit

RMON Group	Support supplied by the unit
Statistics	One default session per segment. All segments and counters are supported.
History	Two default sessions per segment: ■ 30 second intervals, 120 historical samples stored ■ 1800 second intervals, 96 historical samples stored
Alarms	No default sessions created. Maximum of 200 alarms per unit.
Hosts	One session per segment. All segments supported.
Hosts Top N	No default sessions created.
Matrix	One session per segment. All segments supported.
Filter	No default sessions created. All segments supported.
Capture	No default sessions created. All segments supported.
Events	There are many default events. They are described in "Default Events" on page 126.

Default Events

Table 12 details the default read-only events for the unit.

Table 12 Default Read-only Events for the Unit

Description of Event
No action
Send trap
Turn port off for 5 seconds, notify network management application
Turn port off, notify network management application
Turn port on, notify network management application
Turn port off for 5 seconds
Turn port off
Turn port on
Swap resilient link pair, notify network management application
Indicate port state change
Indicate port entering jabber
System started
Software upgrade report
Capability upgraded
Capability downgraded

D SERIAL UPDATE UTILITY

The *Serial Update Utility* (also known as the *Management Agent Upgrade Utility*) can be used to update the Management Agent of selected SuperStack® II units. The CD-ROM supplied with the unit has the latest version of the utility on it.

You would only use this utility if a previous software update has failed and you are unable to communicate with your hubs using the management interfaces. At all other times you should use the management interfaces to update your units.

If you have any problems using the *Serial Update Utility*, refer to "Solving Problems With the Serial Update Utility" on page 129.

Using the Update Utility

The update utility works from an MS-DOS prompt, and it updates one unit at a time. Updating a unit may take several minutes.

To updateupdate the management software of a unit:

1 Connect the serial (COM) port of your PC to the console port of the unit using a null modem cable.

2 If you are using Microsoft Windows 3.1 or earlier, close it down so that you are at the MS-DOS prompt. If you are using Windows 95 or 98, open an MS-DOS window.

3 At the MS-DOS prompt:

a Create a directory called 'update' in the root directory of your PC's hard drive.

b Copy the contents of the '\agent\update\' directory on the CD-ROM to the 'update' directory on the hard drive.

c Copy the management software file to the 'update' directory on the hard drive.

d Change your directory to the 'update' directory on the hard drive.

4 At the MS-DOS prompt, enter the update command:

```
update <file>
```

<file> is the name of the management software file. Note that the software files have the format zzzxx_yy.bin, where:

- zzz is an abbreviation for the unit. For example:

  dsh = Dual Speed Hub

  psh = PS Hub 40

  psf = PS Hub 50

  s2s = SuperStack II Switch

- xx_yy is the version number

CAUTION: *You must use the zzzxx_yy.bin format, otherwise the update fails.*

You can also use the following parameter with the update command to specify the serial (COM) port to use for the PC (COM 1) or (COM 2) — the default for this is COM 1:

`-c 1` or **`-c 2`**

An example of the update command with this parameter is:

```
update -c 1 s2sxx_yy.bin
```

5 Power-down the unit.

6 At your PC, press [Return].

7 Power-up the unit immediately (within 5 seconds).

The utility transfers the management software to the unit.

When the management software has been transferred, your PC displays the following message:

```
Update completed successfully.
  Update another unit? (y/n)
```

8 If you want to update the management software of another unit, enter **y** (for yes), otherwise, enter **n** (for no).

Solving Problems With the Serial Update Utility

If you have any problems using the update utility, use the following actions to solve your problems.

An error occurs when the utility attempts to connect through the serial port of the PC.

Meaning: The serial port being used is not the same as the serial port specified in the update command.

Action: Retry the command ensuring that you specify a value of '1' or '2' for the serial port.

An error occurs when the utility attempts to communicate with the unit.

Meaning: There could be a number of reasons for this:
The unit is not being powered-up within 5 seconds of pressing [Return] (step 7 in the update procedure).

The null modem cable is not connected to the console port of the unit.

The null modem cable is not connected to the serial port of the PC, or, the serial port being used is not the same as the serial port specified in the update command.

The unit is not being powered-off and on as directed.

Action: Retry the command ensuring that you follow all the steps.

An error occur when the utility attempts to open the Management Software file for reading.

There could be two reasons for this:

Meaning: The file specified in the update command does not exist or is in a different directory to the one given.

Action: Check the filename and its location.

Meaning: You do not have read access for the file.

Action: Check the properties of the file using Explorer (in Windows 95 or 98) or File Manager (in other versions of Windows).

The error message `USAGE: update [-c comport] filename` **is displayed.**

Meaning: You are not specifying the correct number of parameters for the update command.

Action: Retry with the correct parameters.

An error occurred when the utility tried to transfer the file.

There could be a number of reason for this:

- The null modem cable has become disconnected from the hub or the PC during the file transfer. Reconnect the cable and start again.
- Power to the hub has been disrupted during the file transfer. Check the power connection to the hub and start again.
- An incorrect file has been specified and transferred to the hub. Check the filenames and start again.
- The utility must be run from MS-DOS. It cannot be used from an MS-DOS Window within Microsoft Windows 3.1.

There are several very uncommon error messages. These are detailed in the readme.txt file in the Agent\Update directory on the CD accompanying the module.

E

Technical Support

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

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

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

This service provides access to online support information such as technical documentation and software, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **`http://knowledgebase.3com.com`**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **`ftp.3com.com`**
- Username: **`anonymous`**
- Password: **`<your Internet e-mail address>`**

You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If you require additional assistance, 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:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- 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 obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590
India	+61 2 9937 5085	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	
Japan	0531 61 6439	From anywhere in	
Malaysia	1800 801 777	S. Korea:	00798 611 2230
New Zealand	0800 446 398	From Seoul:	(0)2 3455 6455
Pakistan	+61 2 9937 5083	Taiwan, R.O.C.	0080 611 261
Philippines	1235 61 266 2602	Thailand	001 800 611 2000
Europe			
From anywhere in	+31 (0)30 6029900 phone		
Europe, call:	+31 (0)30 6054396 fax		
Europe, South Africa, and Middle East			
From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Middle East	1800 9453794
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 3111206
France	0800 917959	Portugal	0800 831416
Germany	0800 1821502	Russia	0800 995014
Hungary	06800 12813	South Africa	0800 995014
Ireland	1800 553117	Spain	900 983125
Israel	1800 9453794	Sweden	020 795482
Italy	1678 79489	Switzerland	0800 55 3072
Luxembourg	0800 3625	U.K.	0800 966197
Latin America			
Argentina	5411 4510 3200	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266		
Colombia	571 629 4827	Peru	800 666 5065
		South America	1800 666 5065

Country	Telephone Number	Country	Telephone Number
North America	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876-3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+ 65 543 6500	+ 65 543 6348
Brazil	5511 523 2725	
Europe, South Africa, and Middle East	+ 31 30 6029900	+ 31 30 6029999
Central and South America	521 201 0075	
From the following countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876 3266	1 408 326 7120 (not toll-free)

GLOSSARY

10BASE-T

This is a technical specification used for Ethernet networks. 10BASE-T is part of the IEEE standards body specification for Ethernet (10Mbps) over Category 3, 4 or 5 twisted pair cable (two pairs of wire — one pair for transmitting data and the other for receiving data). 10BASE-T has a distance limit of approximately 100m (328ft) per segment.

100BASE-TX

This is a technical specification used in Fast Ethernet networks. 100BASE-TX is part of the IEEE standards body specification for 100Mbps (Fast Ethernet) Category 5 UTP (unshielded twisted pair) or STP (shielded twisted pair) cable (two pairs of wire — one pair for transmitting data and the other for receiving data).

auto-sensing

The ports on the Dual Speed Hub 500 are 10/100 auto-sensing, which means that they auto-sense the speed of the connected equipment. See also *Smart auto-sensing*.

bandwidth

Information capacity, measured in bits per second (bps), that a channel can transmit. The bandwidth of Ethernet is 10Mbps.

baud

This is the *signalling* rate of a line, in other words, the rate at which data travels along a line. Baud is the number of transitions (voltage or frequency changes) made per second.

BOOTP

The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

broadcast

A message sent to all destination devices on the network.

broadcast storm

Multiple simultaneous broadcasts that typically absorb available bandwidth and can cause network failure.

cascaded segments

The segments that run up and down the stack by the cascade cables, to which the Dual Speed Hub 500 units' 10Mbps and 100Mbps internal segments connect (or are isolated from).

console port

The port on the Dual Speed Hub 500 accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation (DEC). Ethernet networks operate at 10Mbps using CSMA/CD (a collision detection mechanism) to run over coaxial, twisted pair and fiber optic cabling.

Fast Ethernet

Fast Ethernet operates at 100Mbps and so has 10 times more bandwidth than Ethernet, enabling it to cope with larger amounts of traffic; this results in operation 10 times faster than Ethernet. Fast Ethernet runs over the various 100BASE (cables), such as 100BASE-TX. Fast Ethernet networks operate at 100Mbps and are based on the 10BASE-T Ethernet CSMA/CD network access method, an extension to the IEEE 802.3 specification.

full duplex

The ability of a device or line to transmit data simultaneously in both directions over the same communications link, potentially doubling the throughput of traffic.

half duplex

The term half duplex is used to describe data transmission that can occur in two directions over the same communications link, in only one direction at a time.

HTTP

HyperText Transfer Protocol. The client/server protocol used to connect servers on the World Wide Web.

Internet

The name given to a public network which spans the world and consists of thousands of pieces of network equipment. If you connect to the Internet, you can communicate with equipment and users across the world. The Internet uses a set of protocols called TCP/IP. The World Wide Web is part of the Internet.

intranet

The name given to a large private network usually based on Internet technology. Many businesses have Intranets so their employees can exchange information between offices in many countries. Employees are often given access to the Internet but the Intranet is protected from external access by ‘firewalls’ (security restrictions imposed on incoming traffic).

IP address

Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX

Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN

Local Area Network. A network of connected computing resources (for example workstations, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

line speed

See *baud rate*.

main port

The port in a resilient link that carries data traffic in normal operating conditions.

MIB

Management Information Base. Stores a device’s management characteristics and parameters. MIBs are used by Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Dual Speed Hub 500 contains its own internal MIB.

multicast

Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

PING

Packet INternet Groper. A utility that sends out requests (and waits for a responses) to a device on your network to test whether it can communicate with that device. You can use PING to ensure that your network connections are good.

protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilience

Tolerance. For example, the Dual Speed Hub cascaded cables make a stack of Dual Speed Hub 500 units resilient because you can power off a unit without it affecting the other units in the stack. You can also build resilience into your network by having extra equipment and cabling that carries your traffic if other equipment and cabling fails. See *resilient link*.

resilient link

A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.

RJ-45

Standard 8-wire connector for IEEE 802.3 10BASE-T networks.

RMON

Remote Monitoring. Subset of SNMP MIB II which allows monitoring and management capabilities by addressing up to 10 different groups of information.

RPS

Redundant Power System. Part of the SuperStack® II product range, provides a backup source of power when connected to the Dual Speed Hub 500.

segments

The separate 10Mbps and 100Mbps networks within a Dual Speed Hub 500 to which the ports connect (depending on what speed they are operating at). The segments can be connected to or isolate from the cascade segments (which extend the segments across other units in the stack).

SLIP

Serial Line Internet Protocol. A protocol which allows IP to run over a serial line connection.

Smart auto-sensing

A feature on the Dual Speed Hub 500 which is an extension to 10/100 auto-sensing. Smart auto-sensing monitors 100Mbps connections and if they are unsuitable and will operate better at 10Mbps, the feature downgrades the connections. See *auto-sensing*.

SmartAgent®

Intelligent management agents in devices and logical connectivity systems that reduce the computational load on the network management station and reduce management-oriented traffic on the network. SmartAgent is a 3Com product.

SNMP

Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end-station operation.

stack

A group of units which are connected together in such a way that they function as a single logical repeater.

standby port

The port in a resilient link that takes over data transmission if the main port in the link fails.

TCP/IP

A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet

A TCP/IP application protocol that provides a virtual terminal service, letting the user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP

Trivial File Transfer Protocol. Allows you to transfer files (for example software upgrades) from a remote device.

Transcend®

3Com's management system used to manage all of 3Com's networking solutions.

UDP

User Datagram Protocol. An internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

URL

Uniform Resource Locator. A URL is a unique address of a Web page. Using just the URL, your Web browser can find Web pages on the World Wide Web.

VT100

A type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.

Web

See World Wide Web.

World Wide Web

The World Wide Web (often known as the ‘Web’) is a global network which is part of the Internet. It is made up of thousands of different ‘Web pages’ and ‘Web sites’ (collections of Web pages) which are inter-linked. These Web pages are electronic pages of text and graphics which can be viewed using a Web browser. Many businesses, non-profit organizations and individuals have created Web pages and sites which cover a wide range of information. All Web pages and sites have a unique URL so that they can be located.

INDEX

3Com Corporation LIMITED WARRANTY

Thus warranty applies to customers located in the United States, Australia, Canada (except Quebec), Ireland, New Zealand, UK, and other English language countries for which a translation into the local language is not provided.

SUPERSTACK® II DUAL SPEED HUB 500

HARDWARE

3Com warrants to the end user (Customer) that this hardware product will be free from defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

Lifetime, for as long as the original Customer owns the product (not transferable to a subsequent end user).

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants to Customer that each software program licensed from it, except as noted below, will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided unless specifically included in the Included Services section. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or 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 or from use of the software product not in accordance with 3Com's published specifications or user manual.

THIS 3COM PRODUCT MAY INCLUDE OR BE BUNDLED WITH (1) THIRD PARTY SOFTWARE, OR (2) 3COM SOFTWARE THAT IS LICENSED "AS IS", THE USE OF WHICH IS GOVERNED BY A SEPARATE END USER LICENSE AGREEMENT. THIS 3COM WARRANTY DOES NOT APPLY TO SUCH THIRD PARTY SOFTWARE OR 3COM SOFTWARE LICENSED "AS IS". FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE OR THE ACCOMPANYING DOCUMENTATION RELATING TO SUCH SOFTWARE.

YEAR 2000 WARRANTY

In addition to the Hardware Warranty and Software Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site, http://www.3com.com/products/yr2000.html, as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com within ninety (90) days of purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase.

Obtaining Warranty Service

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a User Service Order (USO) number (or a Return Material Authorization (RMA) number or Service Repair Order (SRO) number, whichever was issued) marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to 3Com until the returned item is received by 3Com. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product, and 3Com will retain risk of loss or damage until the item is delivered to Customer.

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 for repair, whether under warranty or not.

Dead-or-Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided prior to 3Com receiving the defective product, but only if Customer provides a purchase order number, credit card number, or other method of payment acceptable to 3Com, to be used if 3Com needs to charge Customer for the replacement, as explained below. The replacement product will normally be shipped not later than three (3) business days after 3Com’s verification of the DOA product, but may be delayed due to export or import procedures. The shipment of a replacement product prior to 3Com receiving the defective product is subject to local legal requirments and may not be available in all locations. When such a replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days of shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

Shipment of a Replacement Prior to 3Com Receiving the Defective Product is provided for five (5) years, after which time it may be available for a specified fee, but in either case only if Customer provides a purchase order number, credit card number, or other method of payment acceptable to 3Com, to be used if 3Com needs to charge Customer for the replacement, as explained below. 3Com will make commercially reasonable efforts to to ship the product not later than five (5) business days after receiving the request for a replacement, but may be delayed due to product availability or export or import procedures. The shipment of a replacement product prior to 3Com receiving the defective product is subject to local legal requirments and may not be available in all locations. When such a replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days of shipment of the replacement, 3Com will charge Customer for the replacement product, at list price. This replacement prior to 3Com receiving the defective product is different from the fee-based Advance Hardware Replacement Service, which is available as a contracted service offering.

Included Services

3Com’s Electronic Support Services, available at no charge, include 3Com Knowledgebase, information on known bugs, documentation, release notes, and publicly available software and firmware upgrades. 3Com reserves the right to modify or cancel this offering at any time, without advance notice.

Telephone Technical Support, with coverage for basic troubleshooting only, will be provided at no additional charge for 12 months form the date of purchase, on a commercially reasonable efforts basis. Telephone support is provided by 3Com only if Customer purchased this product directly from 3Com, or if Customer’s reseller is unable to provide telephone support. To qualify for this telephone technical support, Customer must register on the 3Com Web site at http://support.3Com.com/index.htm and state the date of purchase, product number, and serial number. 3Com’s response to a request for telephone technical support will be in the form of a return call froma 3Com representative by close of business the following business day, defined as 9 a.m. to 5 p.m, local time, Monday through Friday, excluding local holidays. Please refer to the Technical Support appendix in the User Guide for telephone numbers.

Software Updates. All software and Firmware upgrades and the latest code for this product downloaded through the 3Com Software Library.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 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 OR MALFUNCTION 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 OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, 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, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. and by the laws of the United States, excluding its conflicts of laws principles. The United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety form application to this Limited Warranty.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95054
(408) 326-5000

3Com reserves the right to modify or cancel this offering at any time, without advance notice. This offering is not available where prohibited or restricted by law.

REGULATORY NOTICES

FCC STATEMENT

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

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

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 du Règlement sur le matériel brouilleur du Canada.

CE STATEMENT (EUROPE)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

VCCI STATEMENT

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

BSMI STATEMENT

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