3Com® OfficeConnect® Managed Gigabit Switch

User Guide

3CDSG8

www.3Com.com
Part Number 10016799 Rev. BA
Published July 2008

3Com Corporation
350 Campus Drive
Marlborough,
MA 01752-3064

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

3Com Corporation 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 and the 3Com logo are registered trademarks of 3Com Corporation.

IIEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.
All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally friendly in all operations. To uphold our policy, we are committed to:
Establishing environmental performance standards that comply with national legislation and regulations.
Conserving energy, materials and natural resources in all operations.
Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.
Ensuring that all products can be recycled, reused and disposed of safely.
Ensuring that all products are labelled according to recognized environmental standards.
Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally friendly, and the inks are vegetable-based with a low heavy-metal content.

ABOUT THIS GUIDE

This guide provides information about the Web user interface for the 3Com® OfficeConnect Managed Gigabit Switch. The *Web interface* is a network management system that allows you to configure, monitor, and troubleshoot your switch from a remote web browser. The Web interface web pages are easy-to-use and easy-to-navigate.

User Guide Overview

This section provides an overview to the *User Guide*. The *User Guide* provides the following sections:

- **Getting Started** — Provides introductory information about the OfficeConnect Managed Gigabit Switch and how it can be used in your network. It covers summaries of hardware and software features.
- **System Information** — Provides information on the configuration of the switch.
- **Statistics** — provides information on the network traffic to and from the switch.
- **System** — Provides information for configuring general system information including the user-defined system name, the user-defined system location, and the system contact person.
- **IP Address** — Provides information on managing the IP address of the switch
- Provides information for configuring general system information including the user-defined system name, the user-defined system location, and the system contact
- **Password** – Provides information on managing the passwords required to interface the web and console interfaces.
- **Tools** – Provides information on restoring the default settings and upgrading the firmware.
- **Port Settings** — Provides information for configuring port settings.
- **Storm Control** – Provides information on how to configure the settings for managing broadcast and multicast packets.
- **Port Mirroring** – Provides information on how to copy incoming packets on multiple ports to a single port.
- **Cable Diagnostics** — Provides information for managing cable diagnostics
- **Trunks** — Provides information for configuring Link Aggregation (trunks) which optimizes port usage by linking a group of ports together to form a single LAG, either manually or using the automatic LACP protocol.
- **Configuring VLANs** — Provides information for configuring VLANs. VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single virtual LAN segment, regardless of the physical LAN segment to which they are attached.
- **Managing 802.1X** — Provides information for configuring access to the switch using an external authentication server.

- **Configuring IGMP Snooping** — Provides information for configuring IGMP Snooping.
- **Configuring Rapid Spanning Tree** — Provides information for configuring Rapid Spanning Tree.
- **Configuring Quality of Service** — Provides information defining Quality of Service, including 802.1p and DSCP.
- **Configuring SNMP** — Provides information for configuring the *Simple Network Management Protocol* (SNMP) which provides a method for managing network devices.

Intended Audience

This guide is intended for network administrators familiar with IT concepts and terminology.

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 Web site:

- http://www.3Com.com

Conventions

Table 1 lists conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information Notice	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.

CONTENTS

1 GETTING STARTED

This chapter contains introductory information about the 3Com® OfficeConnect Managed Gigabit Switch (hereafter called the Switch) and how they can be used in your network. It covers summaries of hardware and software features and also the following topics:

- About the OfficeConnect Managed Gigabit Switch
- Front Panel Detail
- LED Status Indicators
- System Specifications
- Installing the Switch
- Setting Up for Management
- Methods of Managing a Switch
- Switch Setup Overview
- Using the Command Line Interface (CLI)
- Setting Up Web Interface Management
- Setting Up SNMP Management V1 or V2
- Default Users and Passwords
- Upgrading Software using the CLI

About the OfficeConnect Managed Gigabit Switch

The OfficeConnect Managed Gigabit Switch is a Gigabit Ethernet switching product that delivers flexible three-speed performance (10/100/1000) and advanced voice-optimized features such as QoS, VLANs and RSTP. This makes the switch ideal for medium businesses and small enterprises seeking to build a secure converged network.

The OfficeConnect Managed Gigabit Switch features the following advantages:

- Full Gigabit speed access ports
- Jumbo frames support
- Port security
- Link aggregation control protocol (LACP)
- Up to 256 VLANs
- Rapid Spanning Tree (RSTP)
- IGMP Snooping
- Port-based mirroring

Summary Of Hardware Features

Table 1 summarizes the hardware features supported by the OfficeConnect Managed Gigabit Switch

Table 1 Hardware Features

Feature	OfficeConnect Managed Gigabit PoE Switch
Addresses	Up to 8,000 supported
Auto-negotiation	Supported on all ports
Forwarding Modes	Store and Forward
Duplex Modes	Half and full duplex on all front panel ports
Auto MDI/MDIX	Supported on all ports. If fiber SFP transceivers are used, Auto MDIX is not supported.
Flow Control	In full duplex operation all ports are supported. The OfficeConnect Managed Gigabit PoE Switch ports are capable of receiving, but not sending pause frames.
Traffic Prioritisation	Supported (using the IEEE Std 802.1D, 1998 Edition). Two traffic queues per port
Ethernet, Fast Ethernet and Gigabit Ethernet Ports	Auto-negotiating 10/100/1000BASE-T ports
SFP Ethernet Ports	Supports fiber Gigabit Ethernet long-wave (LX) and fiber Gigabit Ethernet short-wave (SX) in any combination
Mounting	Can be wall mounted

Front Panel Detail

Figure 1 shows the front panel of the OfficeConnect Managed Gigabit Switch unit.

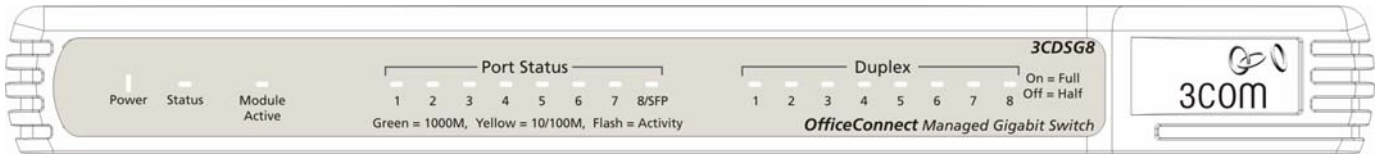


Figure 1: OfficeConnect Managed Gigabit Switch Front Panel

LED Status Indicators

The OfficeConnect Managed Gigabit Switch provides LED indicators on the front panel for your convenience to monitor the switch. Table 2 describes the meanings of the LEDs.

Table 2 Description of the LEDs of the OfficeConnect Managed Gigabit Switch

LED	Label	Status	Description
Power	Power	Green	The power adapter is providing power to the switch
		OFF	The power adapter is not connected correctly or has failed.
System	System	Green	The switch is operating normally. Flashes green when the switch is performing power-on self test (POST) or upgrading firmware.
		Yellow	The switch has failed POST or the software image is corrupt. Consult troubleshooting section.
SFP Module Active	Module Active	Green	The SFP module is inserted and recognised.
		OFF	The SFP module is inserted without link, no SFP module is inserted or the SFP module is not recognized
10/100/1000 BASE-T Ethernet Port Status	Port Status	Green	The port is connected at 1000Mbps. The LED flashed when traffic is transmitted or received.
		Yellow	The port is connected at 10 or 100Mbps. The LED flashed when traffic is transmitted or received.
		OFF	The port is not connected
SFP Ethernet Port Status	Port Status 8/SFP	Green	The SFP module has a valid link. The LED flashed when traffic is transmitted or received.
		OFF	The SFP Module has no link.
Duplex Mode	Duplex	Yellow	The port is in full duplex
		OFF	The port is not connected, or is connected at half duplex.

System Specifications

Table 3 contains the system specifications of the OfficeConnect Managed Gigabit series switch.

Table 3 System specifications of the Switch OfficeConnect Managed Gigabit series switch

Specification	Switch OfficeConnect Managed Gigabit 3CDSG8
Physical dimensions	225 x 135 x 27 mm (8.9 x 5.3 x 1.06 in.)
Weight (Unpackaged)	0.57 kg (1.25 lb)
Console port	One RJ-45 Console port
Gigabit Ethernet ports	8 × 10/100/1000 Mbps Ethernet ports including one shared dual personality Gigabit SFP port
DC Input voltage	Rated voltage range: 12V DC, 1A maximum
Power consumption	23.9 BTU/hr (7.6 Watts)
Operating temperature	0 to 40 °C (32 to 113 °F)
Relative humidity	10 to 90% non-condensing

Additional specifications can be found in Chapter 14 “Device Specifications and Features”

Installing the Switch

This section contains information that you need to install and set up your 3Com switch.

WARNING: Safety Information. *Before you install or remove any components from the Switch or carry out any maintenance procedures, you must read the* 3Com Switch Family Safety and Regulatory Information *document enclosed.*

AVERTISSEMENT: Consignes de securite. *Avant d'installer ou d'enlever tout composant de Switch ou d'entamer une procedure de maintenance, lisez les informations relatives a la securite qui se trouvent dans* 3Com Switch Family Safety and Regulatory Information.

VORSICHT: Sicherheitsinformationen. *Bevor Sie Komponenten aus dem Switch entfernen oder den Switch hinzufugen oder Instandhaltungsarbeiten verrichten, lesen Sie die* 3Com Switch Family Safety and Regulatory Information.

ADVERTENCIA: Informacion de seguridad. *Antes de instalar o extraer cualquier componente del Switch o de realizar tareas de mantenimiento, debe leer la informacion de seguridad facilitada en el* 3Com Switch Family Safety and Regulatory Information.

AVVERTENZA: Informazioni di sicurezza. *Prima di installare o rimuovere qualsiasi componente dal Switch o di eseguire qualsiasi procedura di manutenzione, leggere le informazioni di sicurezza riportate* 3Com Switch Family Safety and Regulatory Information.

OSTRZEŻENIE: Informacje o zabezpieczeniach*. Przed instalacją lub usunięciem jakichkolwiek elementów z product lub przeprowadzeniem prac konserwacyjnych należy zapoznać się z informacjami o bezpieczeństwie zawartymi w* 3Com Switch Family Safety and Regulatory Information.

CAUTION *Opening the switch or tampering with the warranty sticker can void your warranty.*

Setting Up For Management

To make full use of the features offered by your switch, and to change and monitor the way it works, you have to access the management software that resides on the switch. This is known as managing the switch. Managing the switch can help you to improve the efficiency of the switch and therefore the overall performance of your network.

This section explains the initial set up of the switch and the different methods of accessing the management software to manage a switch. It covers the following topics:

- Methods of Managing a Switch
- Switch Setup Overview

- Manually set the IP Address using the Console Port
- Viewing IP Information using the Console Port
- Setting Up Web Interface Management
- Default Users and Passwords

Methods of Managing a Switch

To manage your switch, you need to use Web Interface Management. In addition, you can use the Command Line Interface through the Console port for basic operations of the switch, including viewing the IP address, upgrading the switch firmware and more. Refer to the "3Com CLI Reference Guide" in Chapter 16

Web Interface Management

Each switch has an internal set of web pages that allow you to manage the switch using a Web browser remotely over an IP network.

Switch Setup Overview

This section gives an overview of what you need to do to get your switch set up and ready for management when it is in its default state. Detailed procedural steps are contained in the sections that follow. In brief, you need to:

- Configure IP information manually for your switch or
- View the automatically configured IP information

CAUTION *To protect your switch from unauthorized access, you must change the default password as soon as possible, even if you do not intend to actively manage your switch. For more information on default users and changing default passwords, see "Password" on page 32.*

IP Configuration

The switch's IP configuration is determined automatically using DHCP, or manually using values you assign

Automatic IP Configuration using DHCP

By default the switch tries to configure its IP Information without requesting user intervention. It tries to obtain an IP address from a DHCP server on the network.

Default IP Address

If no DHCP server is detected, the switch will use its default IP information. The default IP address is 169.254.x.y, where x and y are the last two bytes of its MAC address.

Note: The switch's default IP address is listed on a label located on the underside of the switch.

If you use automatic IP configuration it is important that the IP address of the switch is static, otherwise the DHCP server can change the switch's IP addresses and it will be difficult to manage. Most DHCP servers allow static IP addresses to be configured so that you know what IP address will be allocated to the switch. Refer to the documentation that accompanies your DHCP server.

You should use the automatic IP configuration method if:

- your network uses DHCP to allocate IP information, or
- flexibility is needed. If the switch is deployed onto a different subnet, it will automatically reconfigure itself with an appropriate IP address, instead of you having to manually reconfigure the switch.

If you use the automatic IP configuration method, you need to discover the automatically allocated IP information before you can begin management. Work through the "IP Setup" Section on page 81.

Manual IP Configuration

When you configure the IP information manually, the switch remembers the information that you enter until you change it again.

You should use the Manual IP configuration method if:

- You do not have a DHCP server on your network, or
- You want to remove the risk of the IP address ever changing, or
- Your DHCP server does not allow you to allocate static IP addresses. (Static IP addresses are necessary to ensure that the switch is always allocated the same IP information.)

For most installations, 3Com recommends that you configure the switch IP information manually. This makes management simpler and more reliable as it is not dependent on a DHCP server, and eliminates the risk of the IP address changing.

To manually enter IP information for your switch, work through the "IP Setup" on page 81.

Using The Command Line Interface (CLI)

You can access the switch through the Console port to manually set the IP address, or to view the IP address that was assigned automatically (for example, by a DHCP server).

For more information about the CLI, refer to "3Com CLI Reference Guide" on page 77.

Connecting to the Console Port

This section describes how to connect to your switch through the Console port.

Prerequisites

- A workstation with terminal emulation software installed, such as Microsoft Hyperterminal. This software allows you to communicate with the switch using the console port directly.
- Documentation supplied with the terminal emulation software.
- The console cable (RJ-45) supplied with your switch.

You can find pin-out diagrams for the cable in Appendix C on page 74.

Connecting the Workstation to the Switch

1. Connect the workstation to the console port using the console cable

To connect the cable:

- Attach the cable's RJ-45 connector to the Console port of the switch.
- Attach the other end of the cable to the workstation.

2. Open your terminal emulation software and configure the COM port settings to which you have connected the cable. The settings must be set to match the default settings for the switch, which are:
    - 38,400 baud (bits per second)
    - 8 data bits
    - no parity
    - 1 stop bit
    - no hardware flow control

Refer to the documentation that accompanies the terminal emulation software for more information.

3. Power up the switch. The Power on Self Test (POST) will be performed. The OfficeConnect Managed Gigabit Switch takes approximately 30 seconds to boot.

Manually set the IP Address using the Console Port

You are now ready to manually set up the switch with IP information using the command line interface.

You need to have the following information:

- IP address
- subnet mask
- default gateway

1. Connect to the switch Console port as described in "Connecting to the Console Port" page 14.
2. The command line interface login sequence begins as soon as the switch detects a connection to its console port. When the process completes, the Login prompt displays.
3. At the login prompt, enter **admin** as your user name and press Return. The Password prompt displays.

4. Press Return. If you have logged on correctly, the menu should be displayed along with a **>** prompt.
5. Enter **IP** and then press Return
6. Enter **DHCP disable** and press Return
7. Enter the address, subnet mask (and default gateway if required) for the switch as follows:

   ```
   setup xxx.xxx.xxx.xxx mmm.mmm.mmm.mmm ggg.ggg.ggg.ggg
   ```

   and press Enter.

   (Note: xxx.xxx.xxx.xxx is the IP address, mmm.mmm.mmm.mmm is the subnet mask of the switch and ggg.ggg.ggg.ggg is the default gateway if used).

The initial setup of your switch is now complete and the switch is ready for you to connect using your chosen Web browser.

Viewing IP Information using the Console Port

This section describes how to view the automatically allocated IP information using the command line interface. The automatic IP configuration process usually completes within one minute after the switch is connected to the network and powered up.

1. Connect to the switch Console port as described in "Connecting to the Console Port" page 14.

The automatic IP configuration process usually completes within one minute.

2. The command line interface login sequence begins as soon as the switch detects a connection to its console port.
3. At the login prompt, enter **admin** as your user name and press Return.
4. At the password prompt, press Return. If you have logged on correctly, **>** is displayed.
5. Enter **IP summary** to view a summary of allocated IP addresses. The following is an example of the display from the Summary command.

   ```
   > IP status
   IP Method: default
   Dynamic Address: 192.168.1.2 Subnet Mask: 255.255.255.0
   Gateway 192.168.1.1
   dhcp Address 192.168.1.1
   >
   ```

The initial set up of your switch is now complete and the switch is ready for you to set up your chosen management method. See "Methods of Managing a Switch" on page 11.

For more information about the CLI, refer to "3Com CLI Reference Guide" on page 77.

If you do not intend to use the command line interface using the console port to perform other functions, you can disconnect the serial cable and close the terminal emulator software.

Setting Up Web Interface Management

This section describes how you can set up web interface management over the network.

Prerequisites

- Ensure you have already set up the switch with IP information as described in "Methods of Managing a Switch" on page 11.
- Ensure that the switch is connected to the network using a Category 5 or 5E twisted pair Ethernet cable with RJ-45 connectors.
- A suitable Web browser.

For the browser to operate the web interface correctly, JavaScript and Cascading Style Sheets must be enabled on your browser. These features are enabled on a browser by default. You will only need to enable them if you have changed your browser settings.

Web Management Over The Network

To manage a switch using the web interface over an IP network:

1. Be sure that you know your switch's IP address. See "IP Configuration" on page 11, and "Viewing IP Information using the Console Port" on page 14.
2. Check that your management workstation is on the same subnet as your switch.
3. Check you can communicate with the switch by entering a **ping** command at the DOS or CMD prompt in the following format:

   `c:\ ping xxx.xxx.xxx.xxx`

(where xxx.xxx.xxx.xxx is the IP address of the switch)

If you get an error message, check that your IP information has been entered correctly and the switch is powered up.

4. Open your web browser and enter the IP address of the switch that you wish to manage in the URL locator, for example, in the following format:

   `http://xxx.xxx.xxx.xxx`

5. At the login and password prompts, enter **admin** as your user name and press Return at the password prompt (or the password of your choice if you have already modified the default passwords).

The main Web interface page is displayed.

Default Users and Passwords

If you intend to manage the switch or to change the default passwords, you must log in with a valid user name and password. The switch has one default user name. The default user is listed in Table 4.

Table 4 Default Users

User Name	Default Password	Access Level
admin	(no password)	Management — The user can access and change all manageable parameters

Use the admin default user name (no password) to login and carry out initial switch setup.

Upgrading the Software Using the CLI

This section describes how to upgrade software to your Switch from the Command Line Interface (CLI).

You will need a TFTP server application to upgrade the software using this method. Please refer to the instructions that accompanied the TFTP application.

Note: You can also upgrade the software using the switch Web user interface. See "Upgrade Firmware" page 33.

1. To download the runtime application file, enter:

   `IP tftpget aaa.aaa.aaa.aaa rrr`

where aaa.aaa.aaa.aaa is the IP address of the TFTP server and rrr is the source runtime filename.

2. To set the switch to boot from the new software you have downloaded, enter the following:

   `system reboot`

3. The system will now reboot the switch.

Accessing the Switch using the 3Com Detect Application

The 3Com Detect application works by automatically locating your Switch, establishing what IP address it is using and then launching your default web browser to connect directly to it.

The application will only locate your switch if it is on the same subnet as the PC on which the application is running. It will not be able to locate your Switch if there is a router between your PC and the Switch. The application is only designed to run on Windows operating systems.

Running the 3Com Detect Application

The 3Com Managed Gigabit Switch CD-ROM contains in addition to the documentation the 3Com Detect Application.

To use 3Com Detect to connect to the web interface of your Switch, do the following:

1. On the computer that is connected to your Switch (either directly or on a network that is on the same subnet), insert the CD-ROM into it's CD drive.

   If you have autorun enabled, you will be presented with a menu showing the contents of the CD-ROM. Select the 3Com Detect Application link to install the utility. Follow the onscreen instructions.

   If the auto-run program does not start, you should browse to your CD-ROM drive, go to the **/switch detect** directory and double click on **setup.exe**. Follow the prompts that will take you through the installation process.

Once installed, the 3Com Detect Application can be accessed from the Windows Start/Programs list.

When the 3Com Detect application starts, you will be see the Welcome Screen (Figure 2).

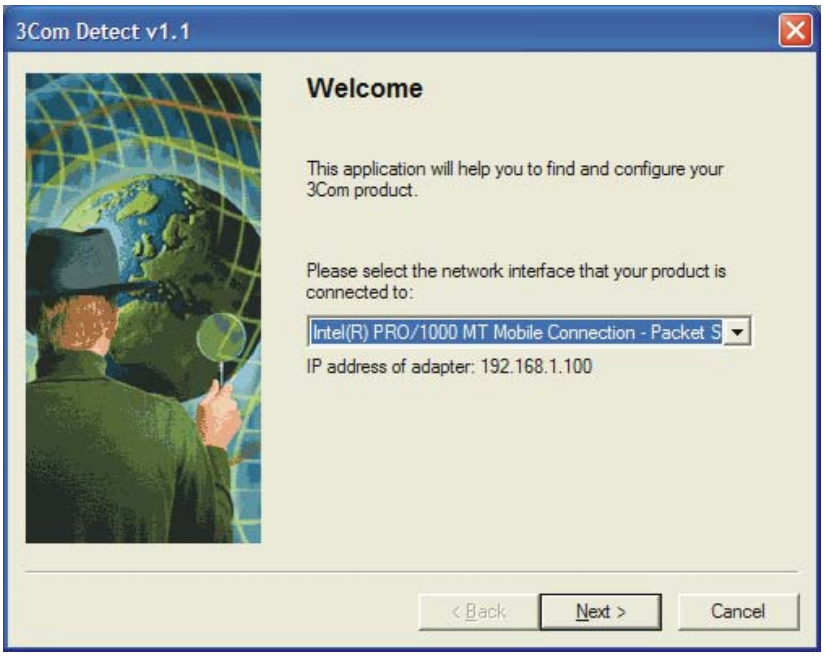
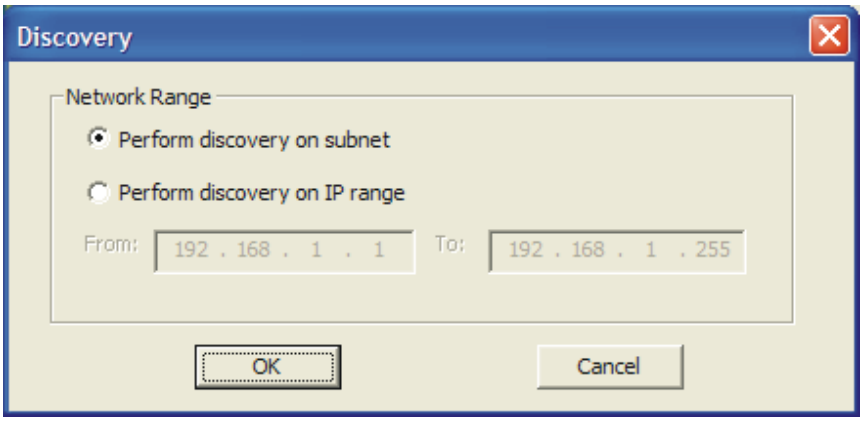


Figure 2: 3Com Detect Welcome Screen

2. If the computer has multiple network adapters, select the adapter that connects the computer to the network or Switch, click "Next".
3. You will then be offered the choice of searching the same subnet that your PC is on for a connected switch (default), or specifying an IP range. Note that specifying a large range may take some time for the search to complete.



4. Once your Switch or Switches have been located you will be presented with a list. Select the switch you wish to connect to and click on "Open". Your default web browser will now open and it will connect to the home page of the Switch.

2 INSTALLING THE SWITCH

This chapter contains information that you need to install and set up the Switch. It covers the following topics:

- Important Safety Information
- Positioning the Switch
- Rack-Mounting or Free-Standing
- Supplying Power to the Switch
- Using SFP Transceivers
- Performing Spot Checks

Important Safety Information
Please refer to the safety information found in the *Support and Safety Information* manual included with this product. You can find the 3Com Switch Family Safety and Regulatory Information manual on the product CD-ROM that was included with your switch. You can also download the safety manual from the 3Com Web site: **www.3Com.com**

Informações Importantes de Segurança
Por favor, antes de manusear o produto, leia cuidadosamente as instruções de segurança encontradas no Manual *Support and Safety Information* incluido no produto. Este manual pode ser encontrado no CD-ROM incluido com o seu switch ou no site da 3Com: **www.3Com.com**

Viktig säkerhets information
Vänligen hänför till säkerhets informationen som är inkluderad med denna produkt i *Support and Safety Information* manualen. Du kan hitta denna manual på den CD-ROM som följde med din switch. Du kan även ladda ner denna från 3Com hemsidan: **www.3Com.com**

Importantes informations de securité
Veuillez consulter les informations de securité qui se trouvent dans le manuel suivant *Support and Safety Information* celui-ci est inclu avec le produit. Vous pouvez trouver ce manuel sur le CD-ROM qui a été livré avec votre switch. Vous pouvez aussi le télécharger sur le site Web de 3Com à: **www.3Com.com**

Wichtige Sicherheits Informationen
Bitte wenden Sie sich an die Sicherheitsinformationen in der *Support and Safety Information* Anleitung die mit diesem Produkt vorhanden ist. Sie können diese Sicherheitsanleitung auf der CD-ROM finden die im Lieferumfang Ihres Netzwerkschalters enthalten ist. Sie können die Anleitungsdatei auch von der 3Com Webseite: **www.3Com.com** herunterladen.

Importante Avviso di Sicurezza
Vi preghiamo di leggere attentamente e seguire le istruzioni indicate nel manuale di sicurezza " *Support and Safety Information* ", che troverete incluso a questo prodotto. Puó trovare il suddetto manuale nel CD-ROM allegato al Vostro Switch. Potete anche scaricarlo dal nostro sito: **www.3Com.com**

Information importante de seguridad

Le rogamos lea y siga atentamente las instrucciones indicadas en el manual de seguridad del *Support and Safety Information*, incluido en este producto. Puede encontrar el manual en el CD-ROM adjunto a su switch. Alternativamente lo puede bajar de la web de 3Com:
www.3Com.com

Istotne informacje dot. bezpiecze stwa
Informacje dotyczące bezpieczeństwa są umieszczone w *Support and Safety Information*, która jest do łączona do tego produktu. Wraz z prze łącznikiem znajduje sie instrukcja na płycie CD-ROM. Istnieje także możliwość pobrania instrukcji bezpośrednio ze strony internetowej
www.3Com.com

Positioning the Switch

The Switch is suitable for use in an office environment where it can be free-standing or wall mounted. When deciding where to position the Switch, ensure that:

- It is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise.

These include lift shafts, microwave ovens, and air conditioning units. Electromagnetic fields can interfere with the signals on copper cabling and introduce errors, therefore slowing down your network.

- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents on the sides of the case are not restricted (3Com recommends that you provide a minimum of 25 mm (1 in.) clearance).
- The air is as free from dust as possible.
- Temperature operating limits are not likely to be exceeded. It is recommended that the unit is installed in a clean, air conditioned environment.

It is always good practice to wear an anti-static wrist strap when installing network equipment, connected to a ground point. If one is not available, try to keep in contact with a grounded rack and avoid touching the unit's ports and connectors, if possible. Static discharge can cause reliability problems in your equipment.

Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Switch from moving around on your desk, or when stacking with flat top OfficeConnect units. Only stick the feet to the marked areas at each corner on the underside of your Switch.

Wall Mounting

There are two slots on the underside of the Switch that can be used for wall mounting. The Switch must be mounted with the LEDs facing upwards.

When wall mounting the unit, ensure it is within reach of the power outlet

When wall mounting the unit, ensure that the rubber feet are not fixed

Mounting Instructions for Cement Walls

1. Make two holes 150 mm (5.9 in.) apart and insert two nylon or similar screw anchors that are suitable for the wall construction.
2. Fix two suitable screws into the anchors, leaving their heads 3 mm (0.12 in.) clear of the wall surface. The screws should be at least 30 mm (1.2 in.) long,
3. Remove any connections in the Switch and locate it over the screw heads. When in line, gently push the Switch on to the wall and move it downwards to secure.

Mounting Instructions for Wood Walls

1. Make two holes 150 mm (5.9 in.) apart.
2. Fix two suitable screws directly into the wall, leaving their heads 3 mm (0.12 in.) clear of the wall surface. The screws should be at least 20 mm (0.75 in.) long,
3. Remove any connections in the Switch and locate it over the screw heads. When in line, gently push the Switch on to the wall and move it downwards to secure.

CAUTION: *When making connections, be careful not to push the Switch up and off the wall.*

Supplying Power to the Switch

Power problems can be the cause of serious failures and downtime in your network. Ensure that the power input to your system is clean and free from sags and surges to avoid unforeseen network outages. 3Com recommends that you install power conditioning, especially in areas prone to blackout, power dips and electrical storms.

Before powering on the Switch, verify that the network cables and the power cable are securely connected.

CAUTION: *The Switch has no ON/OFF switch. The only way to power on and power off the Switch is by connecting and disconnecting the power cord. This is called "power cycling".*

To power on the Switch:

1. Plug the DC power cord from the power adapter into the power socket on the rear panel of the Switch.
2. Plug the power adapter into a power outlet.

When the Switch is powered on, the Power LED lights up. If the Power LED does not light up, check the power supply connections including another mains outlet if appropriate. If the Power LED is still not lit it is likely that the power adapter is faulty. Refer to the Troubleshooting Appendix of this User Guide.

Checking for Correct Operation

After you power on the Switch, it automatically performs a power-on self-test (POST). During POST, the Status LED on the front panel of the Switch flashes green.

When POST is complete, the Status LED turns green. If the Status turns yellow after POST, it means that POST failed and the switch is unlikely to be fully functional. You should reload the software via the console port and restart the switch. If this has not resolved the failure contact your 3Com network supplier for assistance.

The following summarizes the possible colors for the Status LED after POST.

Table 5 Power LED POST Indications

Status	Meaning
Green	The unit is powered on and ready to use.
Yellow	Power-on self-test failed. The Switch is in fail-safe mode. This can happen if a port or ports fail when the Switch was powered on.
Off	The unit is not receiving power: • Verify that the power cord is connected correctly, and then try powering on the Switch again • If the Switch still does not operate, contact your 3Com network supplier

If POST fails, try the following:

- Power off the Switch, and then power it on again. Check the Status LED and see if POST was successfully completed.
- Restore the default configuration the Switch. Refer to the CLI commands appendix for instructions on using the **System Restore Default** command
- Reload the software.

CAUTION: *Resetting the Switch to its factory defaults erases all your settings. You will need to reconfigure the Switch after you reset it.*

If these do not resolve the issue:

- Check the 3Com Knowledgebase for a solution. To visit the 3Com Knowledgebase Web site, start your Web browser, and then enter **http://knowledgebase.3Com.com.**
- Contact your 3Com network supplier for assistance.

Using SFP Transceivers

The following sections describe how to insert an SFP transceiver into an SFP slot.

SFP transceivers are hot-insertable and hot-swappable. You can remove them from and insert them into any SFP port without having to power down the Switch.

Approved SFP Transceivers

The following list of approved SFP transceivers is correct at the time of publication:

- 3CSFP91 SFP (SX)
- 3CSFP92 SFP (LX)

To access the latest list of approved SFP transceivers for the Switch on the 3Com Web site, enter this URL into your Internet browser:

http://www.3Com.com

3Com recommends using 3Com SFPs in the Switch. If you insert an SFP transceiver that is not supported, the Switch will not recognize it.

Inserting an SFP Transceiver

To be recognized as valid, the SFP transceiver must have the following characteristics:

- 1000BASE-SX or 1000BASE-LX media type:
    - 1000BASE-SX SFP transceiver
      Use this transceiver to connect the Switch directly to a multimode fiber-optic cable.
    - 1000BASE-LX SFP transceiver
      Use this transceiver to connect the Switch directly to a single mode fiber-optic cable or to multimode fiber using a conditioned launch cable.

If the SFP transceiver is faulty, it will not operate within the Switch. Non-3Com SFPs may not be recognised

To activate the SFP port:

1. Hold the transceiver so that the fiber connector is toward you and the product label is visible. Ensure the wire release lever is closed (in the upright position).
2. Gently slide the transceiver into the SFP slot until it clicks into place.

CAUTION: *SFP transceivers are keyed and can be properly inserted only one way. If the transceiver does not click when you insert it, remove it, turn it over, and reinsert it.*

3. Remove the plastic protective cover, if fitted.
4. Connect the fiber cable.
5. Attach a male duplex LC connector on the network cable into the duplex LC connector on the transceiver.
6. Connect the other end of the cable to a device fitted with an appropriate Gigabit Ethernet connection.
7. Check the Module Active LED on the front of the Switch to ensure that the SFP transceiver is operating correctly.

Removing an SFP Transceiver

Removing an SFP transceiver does not require powering off the Switch.

To remove an SFP transceiver:

1. Disconnect the cable from the transceiver.
2. Move the wire release lever downwards until it is pointing toward you.

3. Pull the wire release lever toward you to release the catch mechanism. The SFP transceiver should slide out easily.

Performing Spot Checks

At frequent intervals, you should visually check the Switch. Regular checks can give you an early warning of a possible failure; any problems can then be attended to when there will be least effect on users. 3Com recommends periodically checking the cabling, including the power adapter and it's connections.

3 STATUS

3.1 System Information

This page provides an overview of the configuration of the switch. There are five different tables on this page:

- **System Identity** - Displays general information about the switch.
- **Address Information** - Displays the IP Address configuration of the switch.
- **Port Information** - Displays the configuration of every port on the switch.

- **VLAN Information** - Displays the membership information for all VLANs.

Note: This page displays an overview of the switch configuration. To change the switch configuration, use the Web Management-Interface pages referenced on this page.

There are two main buttons associated with this page:

- **HELP** - Displays this window.
- **REFRESH** - Refreshes the page with the current switch configuration and status information.

3.1.1 System Identity

This section contains general information about the switch. **System Name, System Location**, and **System Contact** are set in the **SYSTEM > Name** page. The **Software Version** changes when a new version of software is updated on the switch from the **SUPPORT > Update Software** page. The **Number of Ports, Hardware Version**, and **Serial Number** values are created when the switch is manufactured and cannot be changed.

3.1.2 Address Information

IP Address, **Subnet Mask** and **Gateway IP Address** are set from the **SYSTEM > IP Address** page. **Management VLAN** and **MAC Address** are fixed during manufacture and are provided here for information.

3.1.3 Port Information

This table contains one row for each port on the switch. Each row is divided into eight columns as follows:

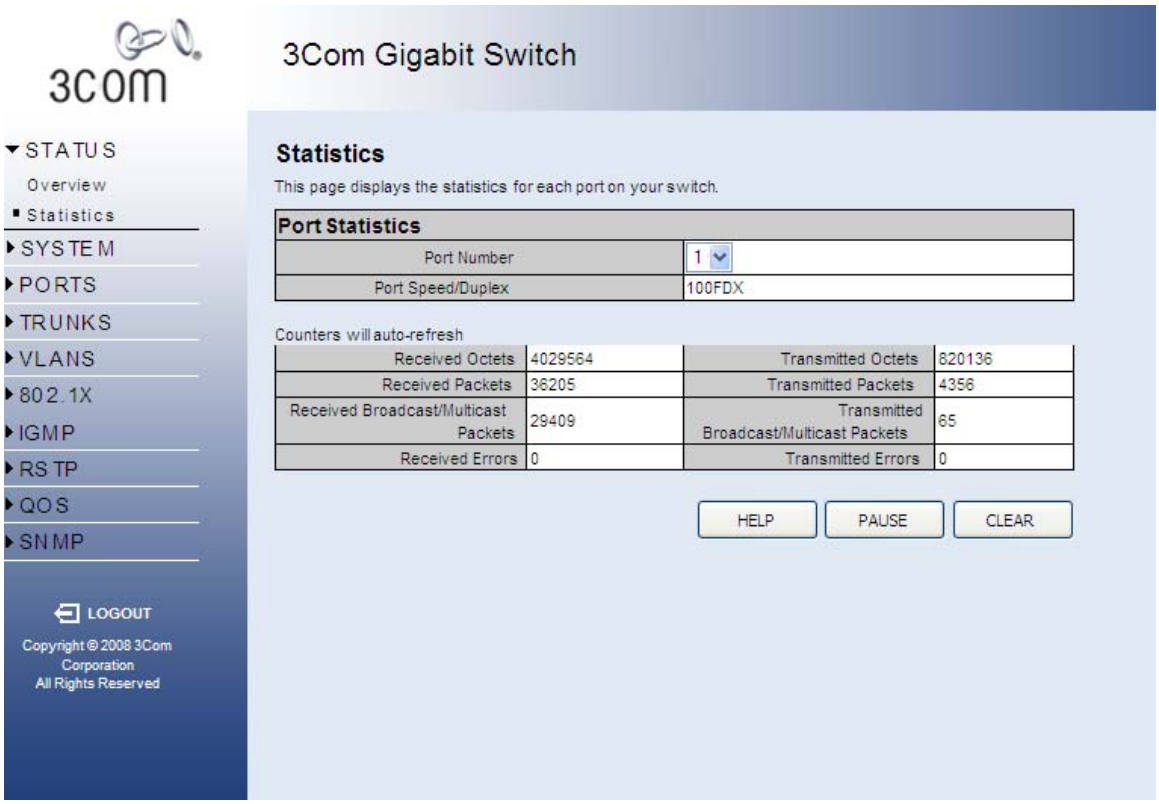
- **Port** - The front-panel port number.
- **Type** - All ports on this switch are 10/100/1000BASE-T.
- **Link Status** - **Up** indicates that the port is connected to another device. **Down** indicates there is no connection. The front-panel "image" that is always visible at the top of the page, also displays this information.
- **Speed/Duplex Status** - An indication of the speed and duplex setting of the port. This is a number, the speed in Mbps, followed by either **FDX** for full-duplex or **HDX** for half-duplex. This can be changed on the **PORTS > Configuration** page.
- **Flow Control Status** - **Enabled** indicates that Flow Control has been enabled on the **PORTS > Configuration** page.
- **Auto-negotiation** - Auto-negotiation is **Enabled** by default and is only **Disabled** when a **Speed/Duplex** setting other than **Auto** is selected on the **PORTS > Configuration** page.
- **Frame Type** - **Tagged** means that the port will only send and receive VLAN-tagged frames. When set to **All** the port will also send and receive untagged packets. See **VLANS > Port Config** for more information.
- **PVID** - The **Port VLAN ID**. When Frame Type is set to **All**, untagged packets arriving on the port will be associated with this VLAN. See **VLANS > Port Config** for more information.

3.1.4 VLAN Information

VLAN 1 will always appear in this table; it cannot be deleted. Other VLANs can be added on the **VLANS > VLAN Setup** page. The two columns in this table are used as follows:

- **VLAN ID** - A number in the range 1 - 4094 which identifies the VLAN.
- **VLAN Members** - A list of the ports that are members of the VLAN. By default, all ports are members of VLAN 1.

3.2 Statistics



You can display statistics on network traffic from the ports. These statistics can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). All values displayed have been accumulated since the last system reboot, but can be reset to zero by clicking the CLEAR button. The current statistics are not displayed until you click the REFRESH button.

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Errors	The number of inbound packets that contained errors preventing

	them from being deliverable to a higher-layer protocol.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received High Priority Packets	The total number of received packets that set as High Priority in the QoS settings.
Transmitted High Priority Packets	The total number of transmitted packets that set as High Priority in the QoS settings.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Normal Priority Packets	The total number of received packets that set as High Priority in the QoS settings.
Transmitted Normal Priority Packets	The total number of transmitted packets that set as High Priority in the QoS settings.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.

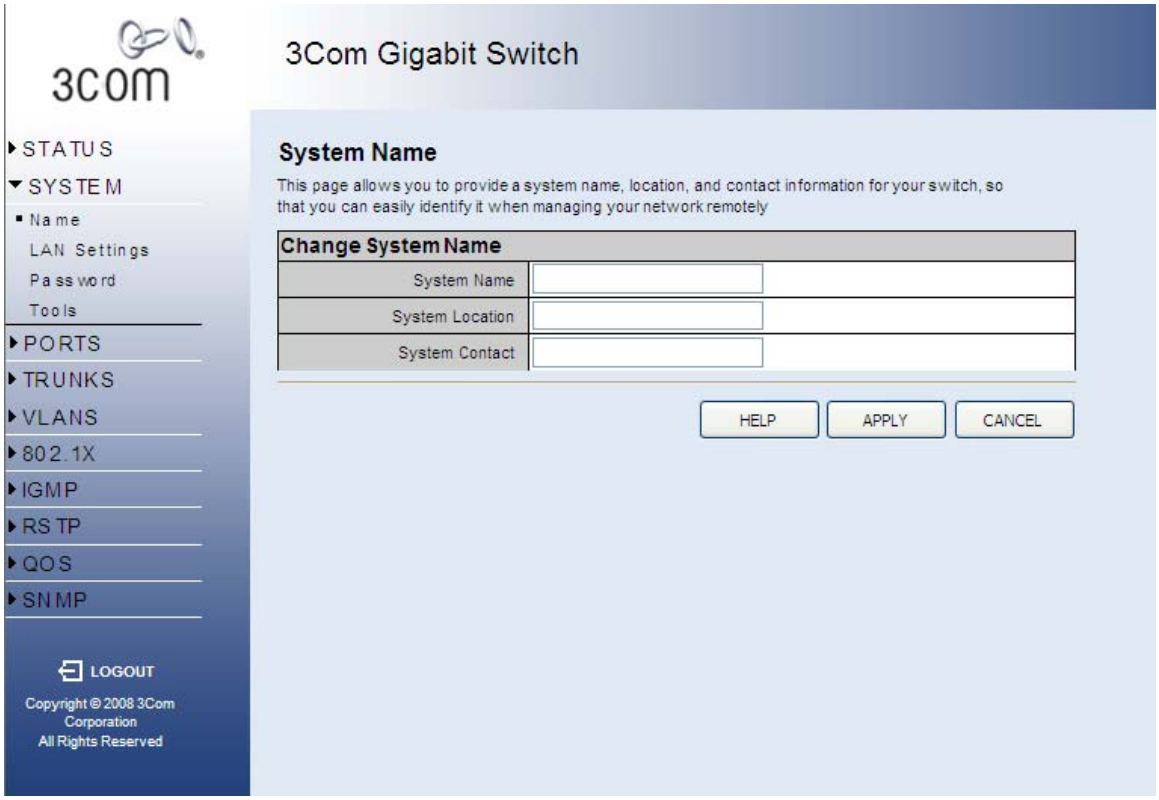
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

There are two main buttons associated with this page:

- **REFRESH** - Resends the information.
- **CLEAR** - Clears all counters and sets them back to zero.

4 SYSTEM

4.1 Name



This page allows you to change the System Name, System Location, and System Contact. The System Name is displayed on the Login page, and the **SYSTEM > Information** page.

- **System Name** - The name of the switch. The System Name can be up to 24 characters long.
- **System Location** - Description of the switch location. The System Location can be up to 24 characters long.
- **System Contact** - The contact name for the switch. The System Contact can be up to 24 characters long.

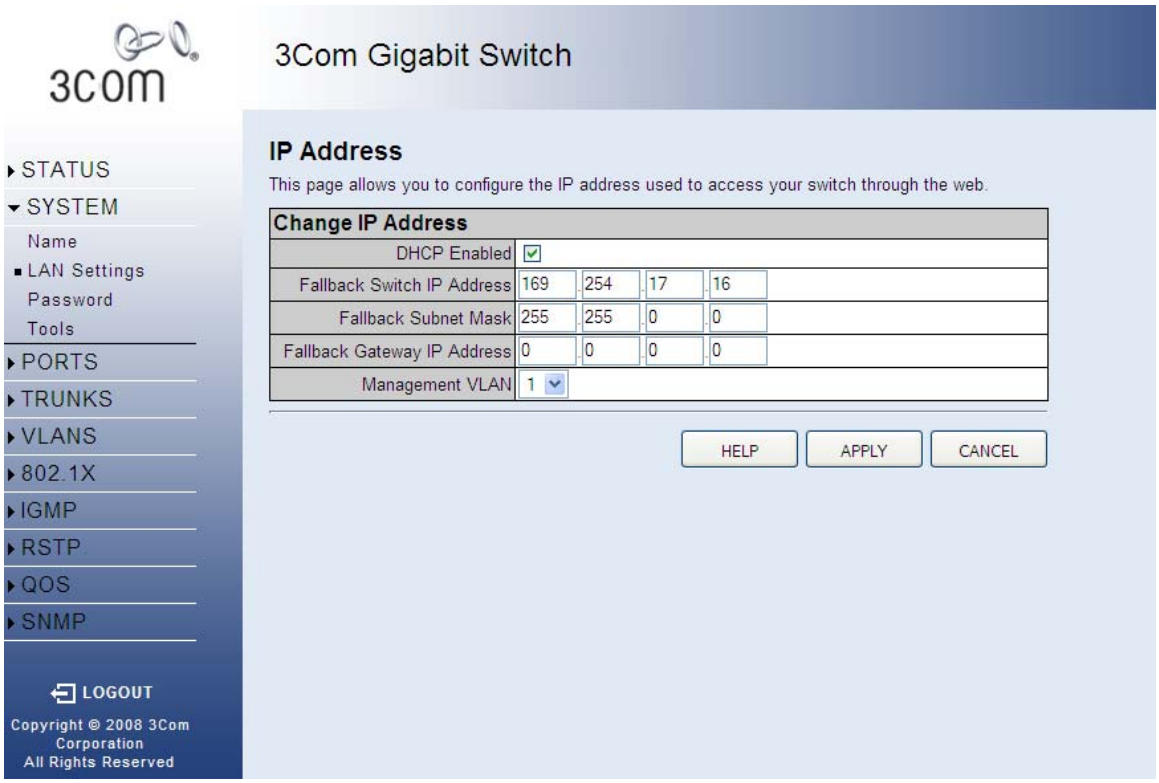
Note: The System Name, System Location, and System Contact will accept all characters on the keyboard (ie: numbers, upper-case and lower-case letters, and keyboard symbols).

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.

- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

4.2 IP Address



This page allows you to change the IP Address used by the switch.

- **DHCP Enabled** - If enabled, the IP Address will be assigned from the DHCP server. If disabled, the IP Address must be assigned manually.
- **Switch IP Address** - The dot-separated IPv4 address used by the switch.
- **Subnet Mask** - The dot-separated IPv4 Subnet address used by the switch. If in doubt, set this to be the same as the Subnet Mask used by your PC.
- **Gateway IP Address** - The dot-separated IPv4 Gateway address used by the switch. If in doubt, set this to be the same as the Default Gateway address used by your PC.

Note: If DHCP is enabled, the word "Fallback" will be added to the front of the other parameter names to indicate the usage of a manually assigned IP Address.

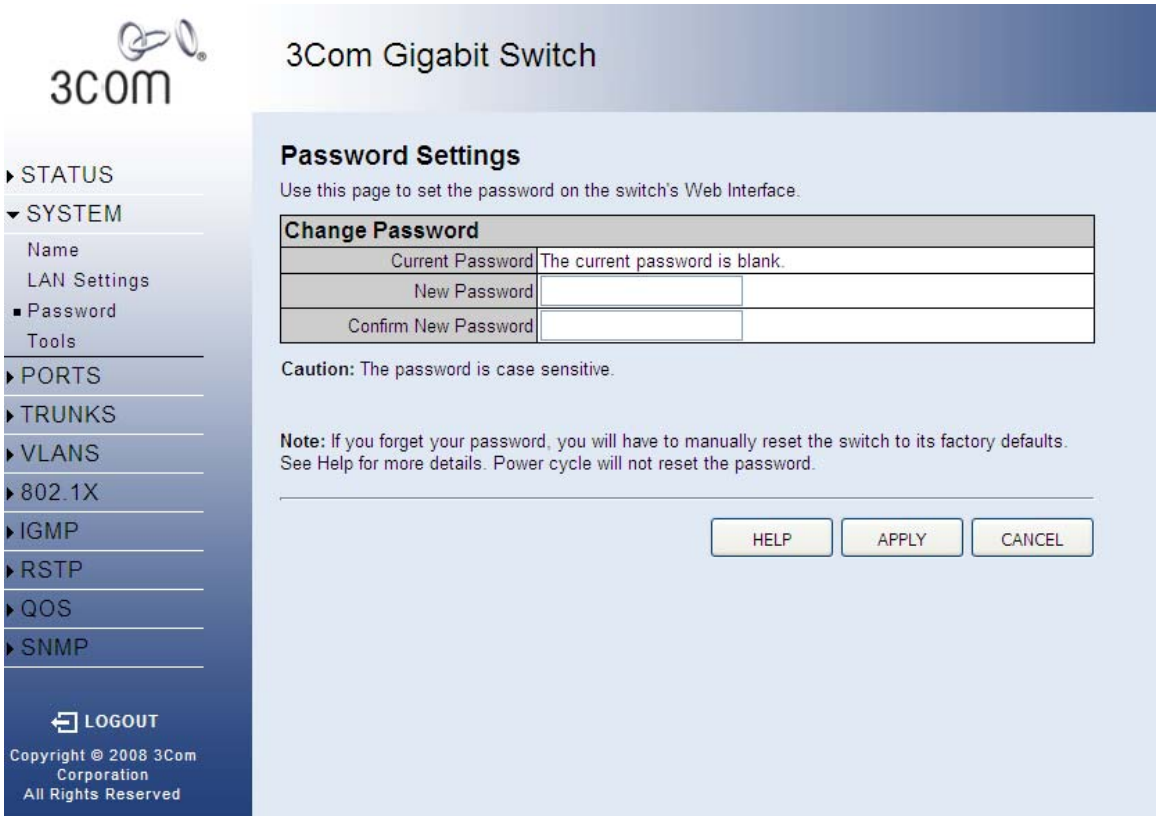
Note: If you change the IP address used by the switch you will lose contact with this Web Management-Interface and may have to change the IP address on your PC to reconnect.

Note: If you forget the IP Address you can connect to the console interface and use the **IPStatus** command to display it. See Page 77 for more details.
There are three main buttons associated with this page:

- **HELP** - Displays this text.

- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

4.3 Password



This page allows you to change the password that is required to access this Web Management-Interface. You will need to enter the following:

- **Current Password** - The password that you used to login to this interface. There is no default password.
- **New Password** - Your new password, up to 16 characters long. Passwords are case-sensitive.
- **Confirm Password** - Re-enter the new password to ensure it has been entered correctly.

Note: Can be up to 16 characters long and can consist of any alphanumeric characters. Passwords are case-sensitive.

Note: It is extremely important that you do not forget your password. If you forget your password, you will have to manually reset the switch to its factory defaults. See the **Troubleshooting** page for more details. Power cycle will not reset the password.

There are three main buttons associated with this page:

- **HELP** - Displays this text.

- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

4.4 Tools

On the Tools page, you can restore the switch to default settings, upgrade the firmware of the switch, or restart the switch.

Restore to Factory Defaults

Forces the switch to restore the original factory settings. To reset the switch, select "Reset to Factory Defaults" from the drop-down list and click APPLY.

Upgrade Firmware

Upgrades the switch system firmware using a file provided by 3com. Select "Upgrade Firmware" from the Tools drop-down list then click on the "Browse" button to select the firmware file. Click the APPLY button to upgrade the selected switch firmware file. You can download firmware files for your switch from the Support section of the 3com web site at www.3com.com.

Upload/Download Configuration

To upload or download the configuration file, select “Upload/Download Configuration” from the Tools drop-down list, then click “Upload” or “Download,” and then click on the “Browse” button to select the file.

Restart Switch

To restart the switch, select from the Tools drop-down list, and then click APPLY. The reset will be complete when the user interface displays the login page.

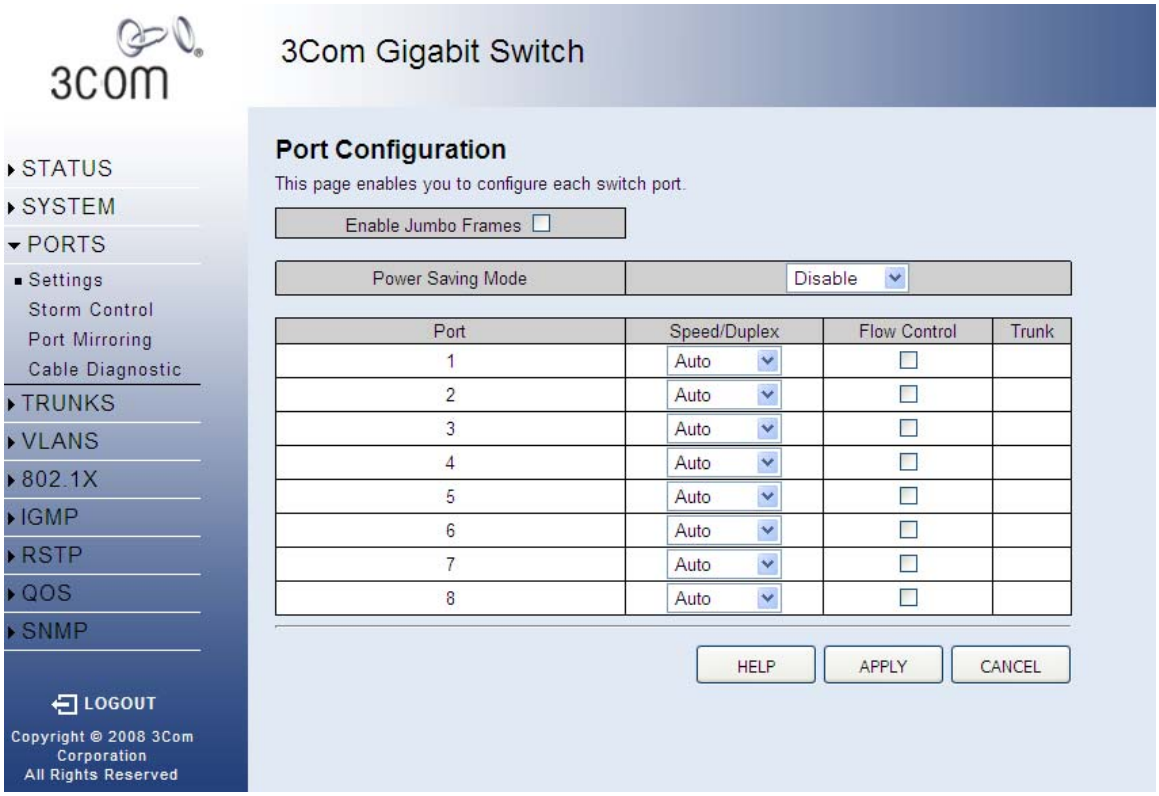
There are two main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **BROWSE** - Navigates to a file.

Note that the **Browse** command is not applicable to all actions on this page, for example **Restart**.

5 PORTS

5.1 Settings



This page allows you to configure Jumbo Frames, Speed, Duplex and Flow Control settings for every port on the switch. It also allows the power saving modes to be configured.

- **Enable Jumbo Frames** - Click box to enable jumbo frames. This setting is applied to all the ports on the switch.

The Port Configuration table has one row for each port and four columns. The columns are:

- **Port** - The front-panel port-number of the port. This cannot be changed.
- **Speed/Duplex** - A combined data-rate and duplex setting for the port.
- **Flow Control** - Used to control congestion and to minimize the number of dropped packets.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

5.1.1 Power Saving Mode

The power saving modes allow the switch to reduce the amount of power it consumes by monitoring the devices connected to the switch. There are two ways in which the switch can save power: Sensing the cable length and powering down un-connected ports.

The Ethernet standard has been designed to operate over cable lengths of up to 100m (328 feet). However in many networks, the cables are much shorter, meaning much of the power required to drive the signal over the full 100m distance is 'wasted'. This OfficeConnect® switch is able to determine the length of the cable between it and the connected device. For short cables below 30m (approx. 98 feet), the switch can reduce the strength of the signal while maintaining correct operation. Between 30m and 70m (approx. 230 feet) the signal amplitude will be increased compared to below 30m operation, but still with a power saving. Above 70m full signal amplitude is applied and there is no power saving.

Note: When enabled, the cable length detection mode will determine the cable length every time a cable is plugged into a port and link is established.

The switch is also able to determine if ports on the switch are unconnected. If this is the case then the switch can power down the port on the switch to save the power that would normally be wasted when no cable was connected. When a device is connected to the switch it will power the port back up to ensure normal operation.

Note: The power saving modes have been rigorously tested to ensure that your OfficeConnect® switch meets and exceeds all the applicable industry standards. When power saving modes are being used you will not detect any loss of performance or reliability. You will be contributing to the important task of reducing global energy consumption.

The Power Saving settings for the switch are set by a single drop-down list. The power saving settings are applied to all ports. The possible values are:

- **Full** – Both cable length detection and port shutdown are enabled
- **Link Up** – Just the cable length detection mode is enabled
- **Link Down** – Just the port shutdown mode is enabled
- **Disabled** – None of the power saving modes are enabled

5.1.2 Speed/Duplex

The Speed and Duplex settings for the port are set by a single drop-down list. The possible values are:

- **Auto** - Speed and duplex settings are auto-negotiated.
- **10HDX** - 10 Mbps, half-duplex
- **10FDX** - 10 Mbps, full-duplex
- **100HDX** - 100 Mbps, half-duplex
- **100FDX** - 100 Mbps, full-duplex
- **1000FDX** - 1000 Mbps, full-duplex

Note: Auto is the default setting and need not be changed unless you are experiencing problems establishing link with a connected device (i.e. the front-panel LEDs or **SYSTEM >**

Information page indicate that the link is down when there is a cable connecting a device to the switch).

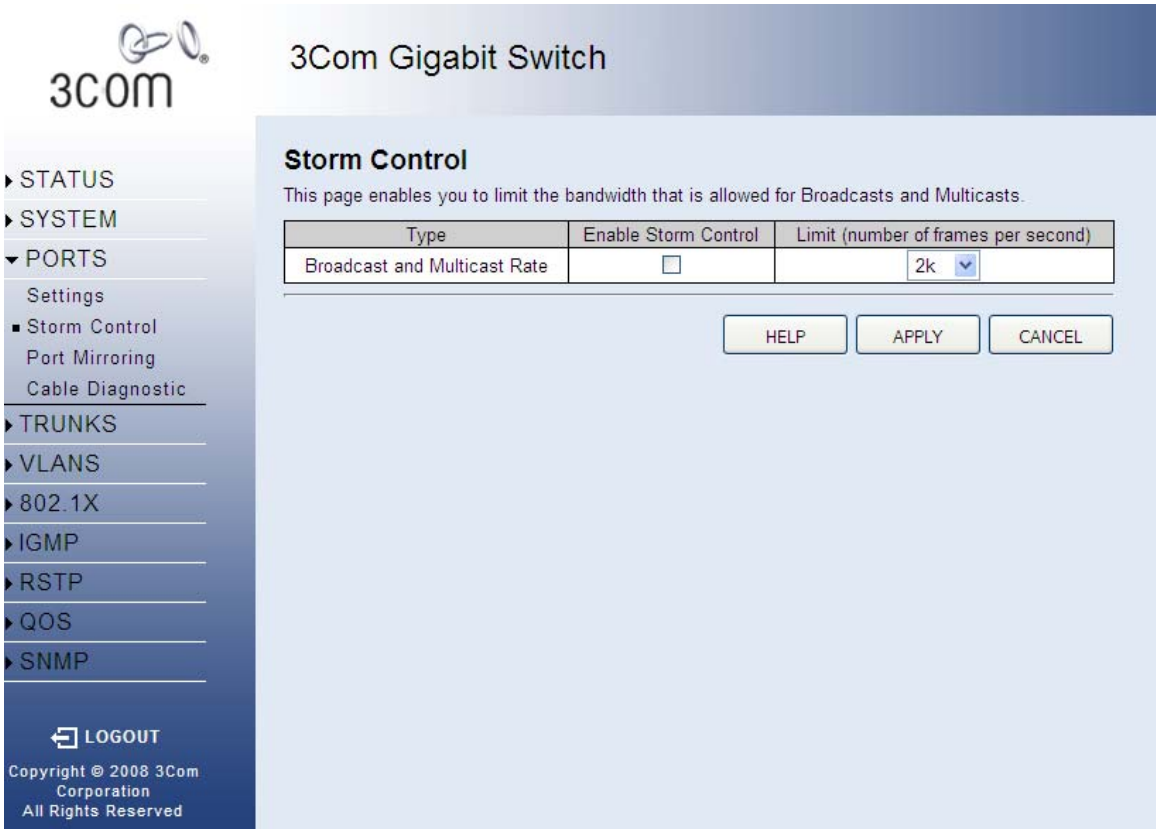
Note: Auto causes the switch to negotiate the link speed and duplex settings with the connected device; this is called Auto-negotiation. All of the other settings cause Auto-negotiation to be turned off.

Note: In full-duplex mode, both ends of a connection can send traffic at the same time which effectively doubles the available throughput. In half-duplex mode, only one end of the connection can send traffic at any one time.

5.1.3 Flow Control

When **Flow Control** is selected on a port (by clicking on the tick-box in the **Flow Control** column), the switch will attempt to slow incoming traffic down when traffic levels are high. It does this by sending special Pause packets on full-duplex connections or creating back-pressure (deliberately causing collisions) on half-duplex connections. This can increase traffic throughput by reducing the number of dropped packets and, as a result, the number of resends that are required. However it is not appropriate in all circumstances.

5.2 Storm Control



This page allows you to set up a threshold for incoming broadcast and multicast packets. Too many incoming packets can severely cripple the switch and network performance. Rate limiting protects the switch and network by keeping the amount of data passing through the ports to a safe limit. The use of VLANs and Trunks to partition ports and network devices into separate

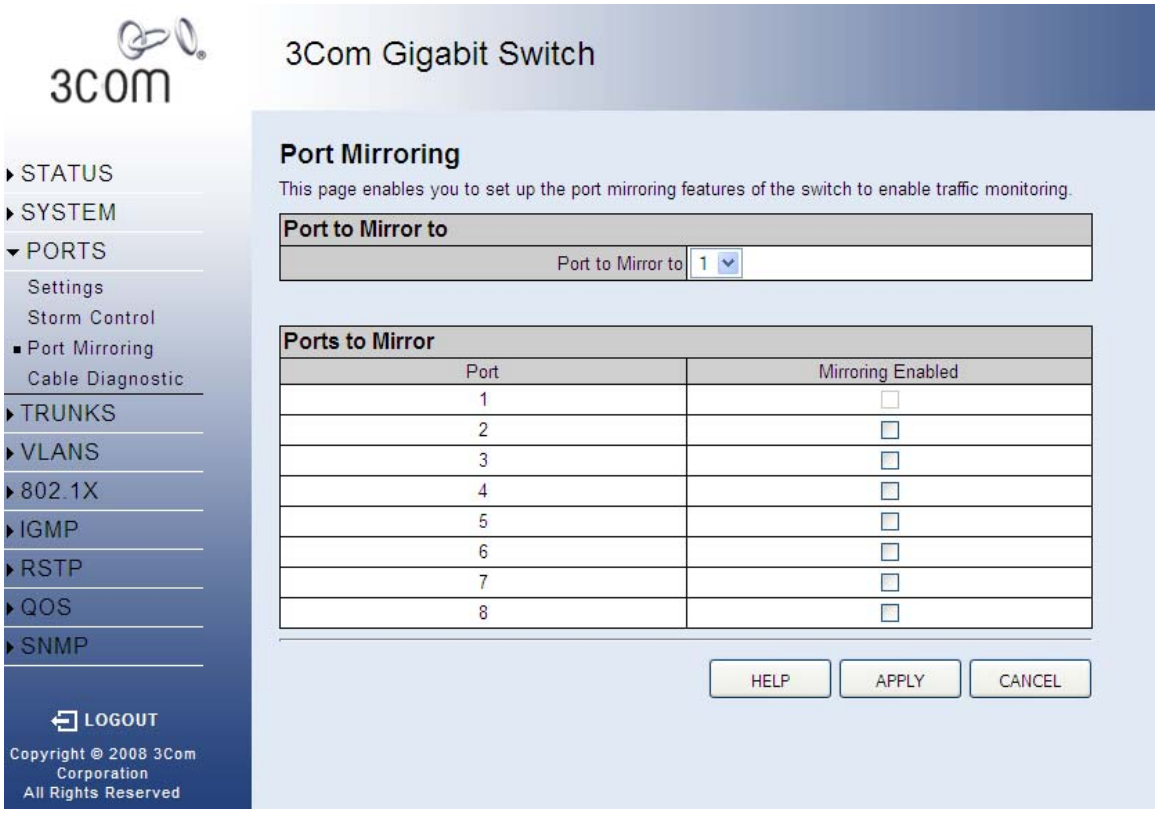
groups can also keep the network from unnecessary traffic by restricting the packet destination. The same setting is applied to all the ports on the switch.

- **Type** – List the type of traffic which can be rate limited, including ICMP, learn frames, broadcast, multicast and flooded unicast frames.
- **Enable Storm Control** – Click the check box to enable storm control for the specific frame type.
- **Rate**(number of frames per second) – The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

5.3 Port Mirroring



This page allows you to copy (mirror) incoming packets on multiple ports to a single port. This can be useful for diagnosing problems. The page is split into two sections:

- **Port to Mirror to** - Choose the destination port. All the mirrored packets will be sent to the selected port.
- **Ports to Mirror** - The front-panel port number.

Note: You cannot mirror the destination port.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

5.3.1 Port to Mirror to

Select the destination port from **the Port to Mirror to** drop-down list. Any port can be selected. The tick-box of the selected port will be cleared and disabled (see the **Ports to Mirror** section).

Note: Broadcast and Multicast packets are not mirrored since they are flooded to all ports anyway.

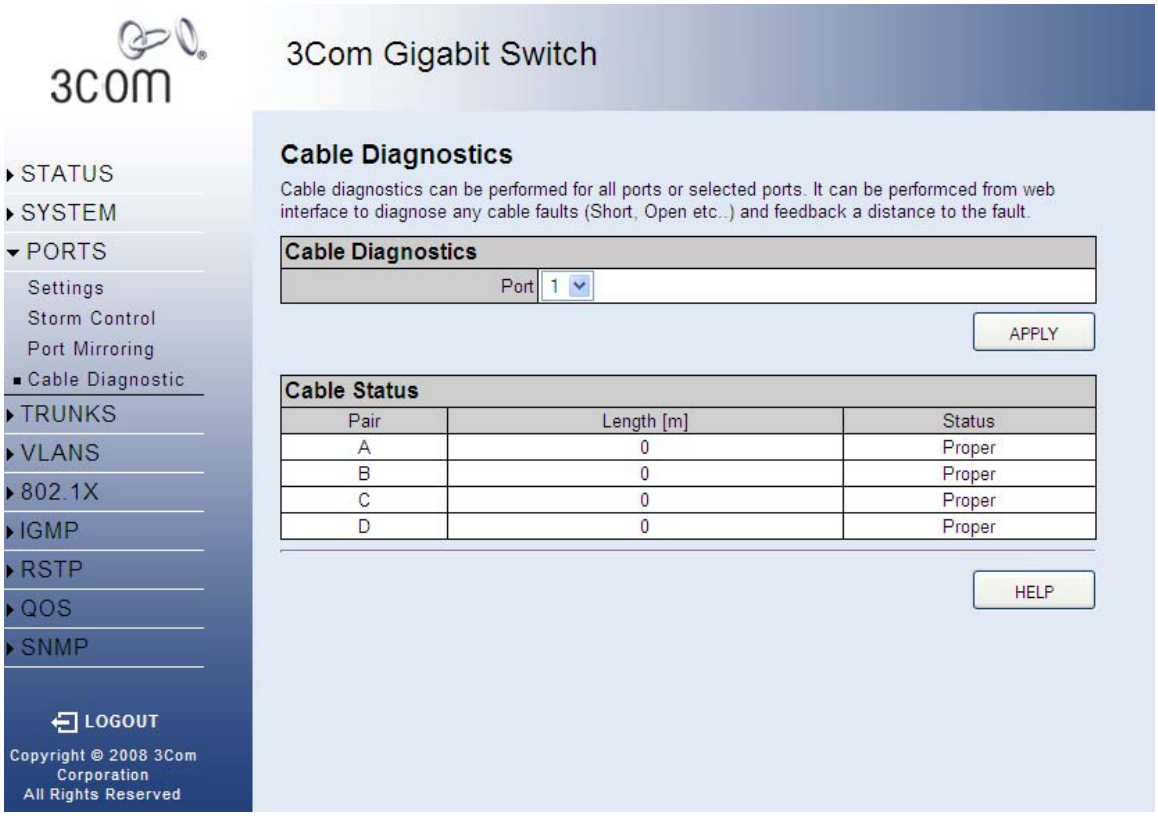
5.3.2 Ports to Mirror

There are four columns in this table. Two are titled **Port** and two are titled **Mirroring Enabled**.

- **Port** - The front-panel port number.
- **Mirroring Enabled** - This field is associated with the port-number that is displayed immediately on its left. Click on the tick-box to enable/disable Port Mirroring for the port.

Note: It will not be possible to select **Mirroring Enabled** for the destination port (the **Port to Mirror to**).

5.4 Cable Diagnostics



You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc..) and feedback a distance to the fault.

- **Cable Diagnostics** – Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.
- **Cable Status** – Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

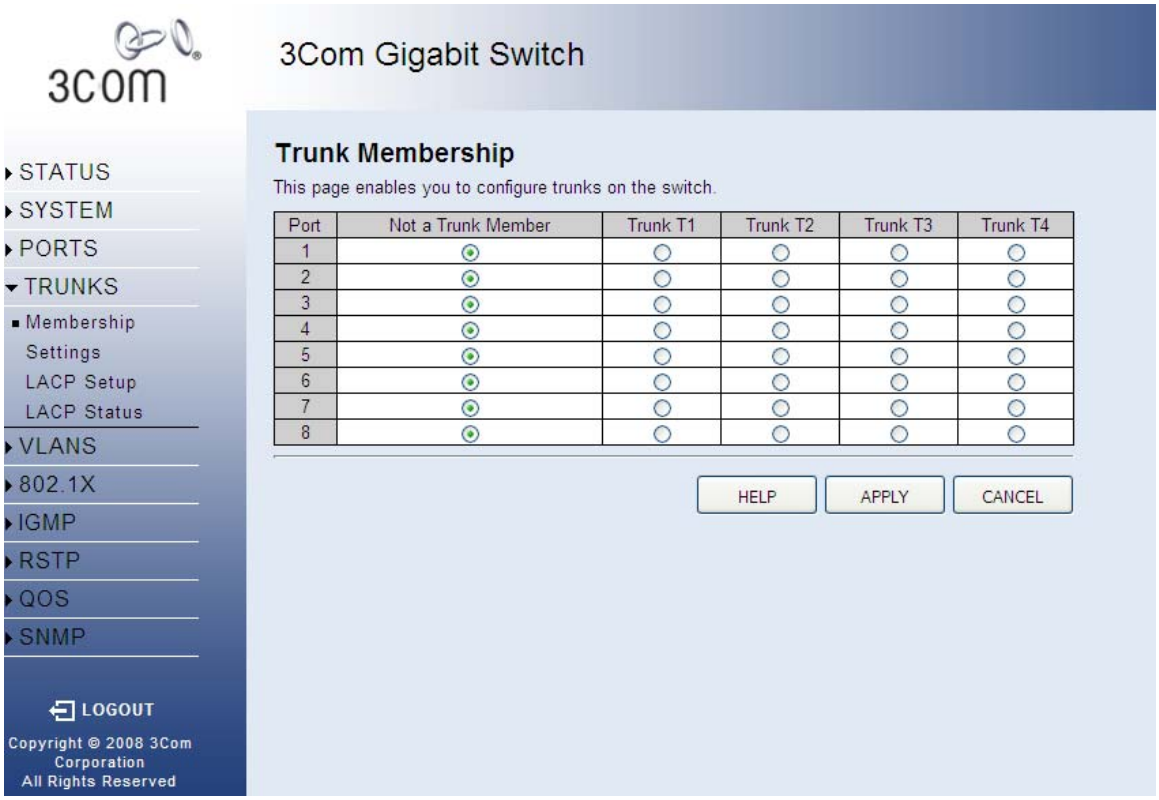
Note: Due to a hardware issue Port 8 cannot display cable diagnostic information.

There are two main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.

6 TRUNKS

6.1 Membership



This page allows you to create a maximum of 4 trunks of up to 8 ports each. For instructions on how to create, modify, and delete trunks, please see **Working with Trunks**.

The Membership Table has one row for each port and a column for each trunk, plus an additional column for ports that are not members of a trunk. Each row contains radio buttons which are used to indicate which trunk (if any) the port belongs to. Each radio button is in a column of its own. The columns are:

- **Port** - The front-panel port number.
- **Not a Trunk Member** - If the radio button in this column is selected, the port is not a member of any trunks. This is the default state.
- **Trunk T1 - T4** - These columns correspond to the 4 trunks that are supported by the switch. Clicking on the radio button in any one of these columns causes the port to become a member of the corresponding trunk. Each trunk can have a maximum of 8 ports, and a minimum of 1 port.

When a trunk is first created it is given the following, default configuration:

- **Speed/Duplex** is set to Auto Speed (see **TRUNKS > Configuration**)
- **Flow Control** is turned off (see **TRUNKS > Configuration**)

- The trunk is a member of **VLAN 1** with a **PVID** of 1. The trunk will accept both tagged and untagged packets (see **VLANS > VLAN Settings**)

Ports that are removed from a trunk, retain the configuration (i.e. Speed, Duplex, and Flow Control) that they had when they were members of the trunk. Ports that are added to the trunk after its creation, inherit the current configuration of the trunk.

You can configure the trunks from the **TRUNKS > Configuration** page.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

6.1.1 Working with Trunks

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices.

To create a trunk or add a port to an existing trunk (from the TRUNKS > Membership page):

1. Under one of the trunk columns (**Trunk T1 to Trunk T4**), click the tick-box of the port you would like to add to the trunk. You can choose a maximum of 8 ports or minimum of 1 port per trunk.
2. Click the APPLY button.

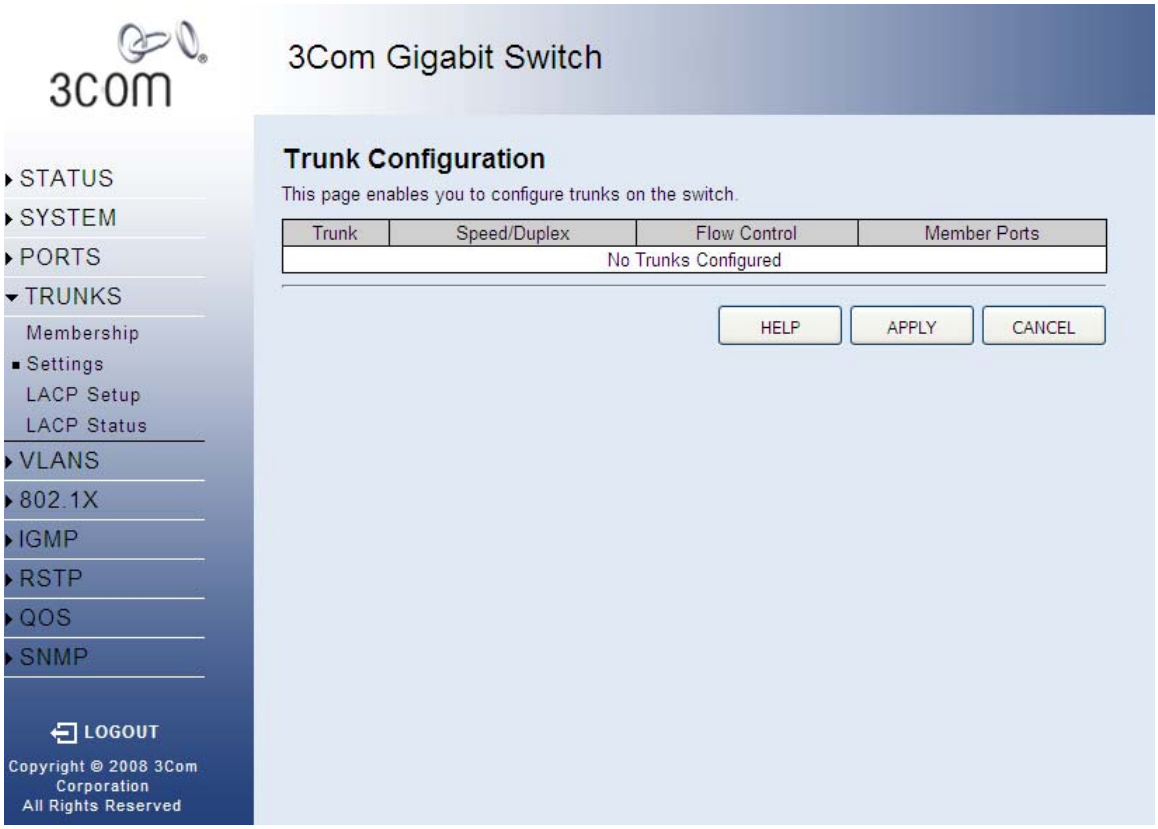
To delete a trunk or remove a port from an existing trunk (from the TRUNKS > Membership page):

1. Under the **Not a Trunk Member** column, click the tick-box of the port you would like to remove from the trunk. If you remove all ports from a trunk then the trunk itself will be deleted.
2. Click the APPLY button.

To configure an existing trunk (from the TRUNKS > Configuration page):

1. From the **Speed/Duplex** drop down menu, you can set the speed and duplex for all the ports in that trunk.
2. Click the **Flow Control** box to enable or disable flow control for all the ports in that trunk.

6.2 Settings



This page allows you to change the Speed, Duplex and Flow Control settings for each trunk on the switch. The **Trunk Configuration Table** has one row for each trunk and four columns.

The columns are:

- **Trunk** - The Trunk Label. Trunks are labeled T1 up to T4.
- **Speed/Duplex** - A combined data-rate and duplex setting for the port.
- **Flow Control** - Used to control congestion and to minimize the number of dropped packets.
- **Member Ports** - The individual ports that go together to make the trunk (i.e. the members of the trunk).

Note: When configuring a trunk, all member ports are configured identically.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

6.2.1 Speed/Duplex

The Speed and Duplex settings for the trunk are set by a single drop-down list. The possible values are:

- **Auto** - Speed and duplex settings are auto-negotiated.
- **10HDX** - 10 Mbps, half-duplex
- **10FDX** - 10 Mbps, full-duplex
- **100HDX** - 100 Mbps, half-duplex
- **100FDX** - 100 Mbps, full-duplex
- **1000FDX** - 1000 Mbps, full-duplex

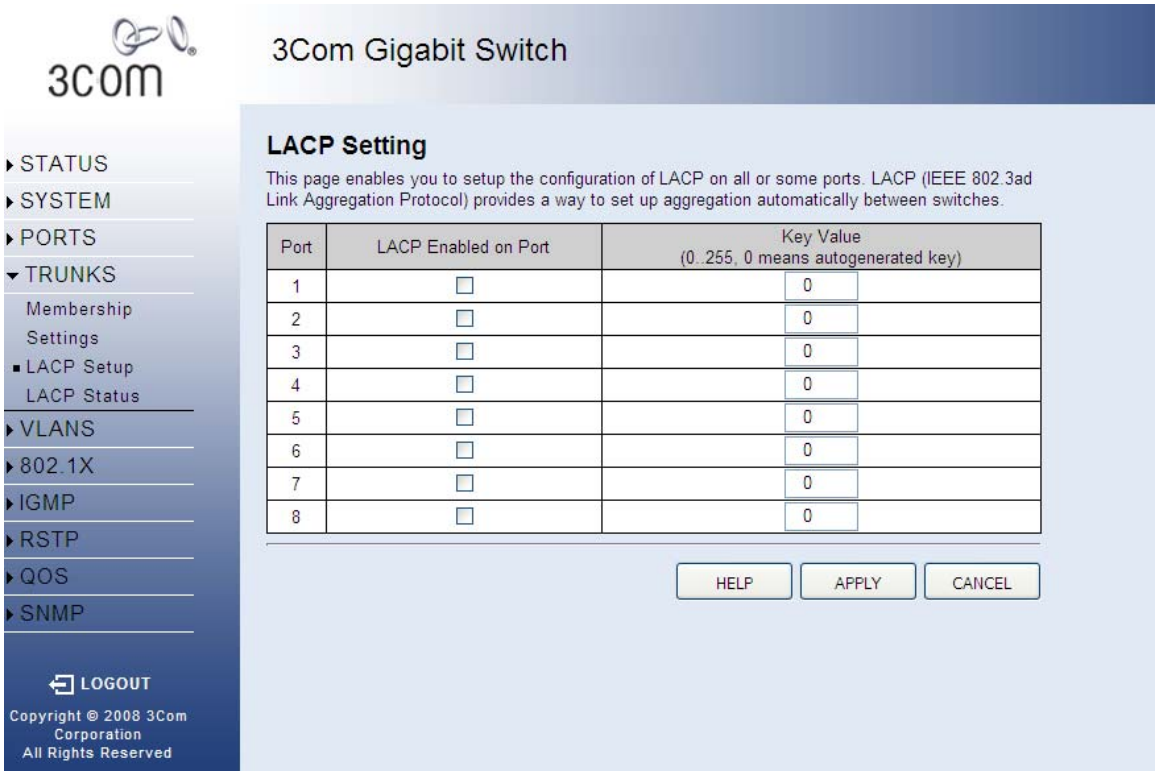
Note: Auto is the default setting and need not be changed unless you are experiencing problems establishing link with a connected device (i.e. the front-panel LEDs or **SYSTEM > Information** page indicate that the link is down when there is a cable connecting a device to the switch).

Note: In full-duplex mode, both ends of a connection can send traffic at the same time which effectively doubles the available throughput. In half-duplex mode, only one end of the connection can send traffic at any one time.

6.2.2 Flow Control

When **Flow Control** is selected on a port (by clicking on the tick-box in the **Flow Control** column), the switch will attempt to slow incoming traffic down when traffic levels are high. It does this by sending special Pause packets on full-duplex connections or creating back-pressure (deliberately causing collisions) on half-duplex connections. This can increase traffic throughput by reducing the number of dropped packets and, as a result, the number of resends that are required. However it is not appropriate in all circumstances.

6.3 LACP Setup



This page allows you to configure LACP for each port. The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it. The LACP Table has one row for each port and three columns.

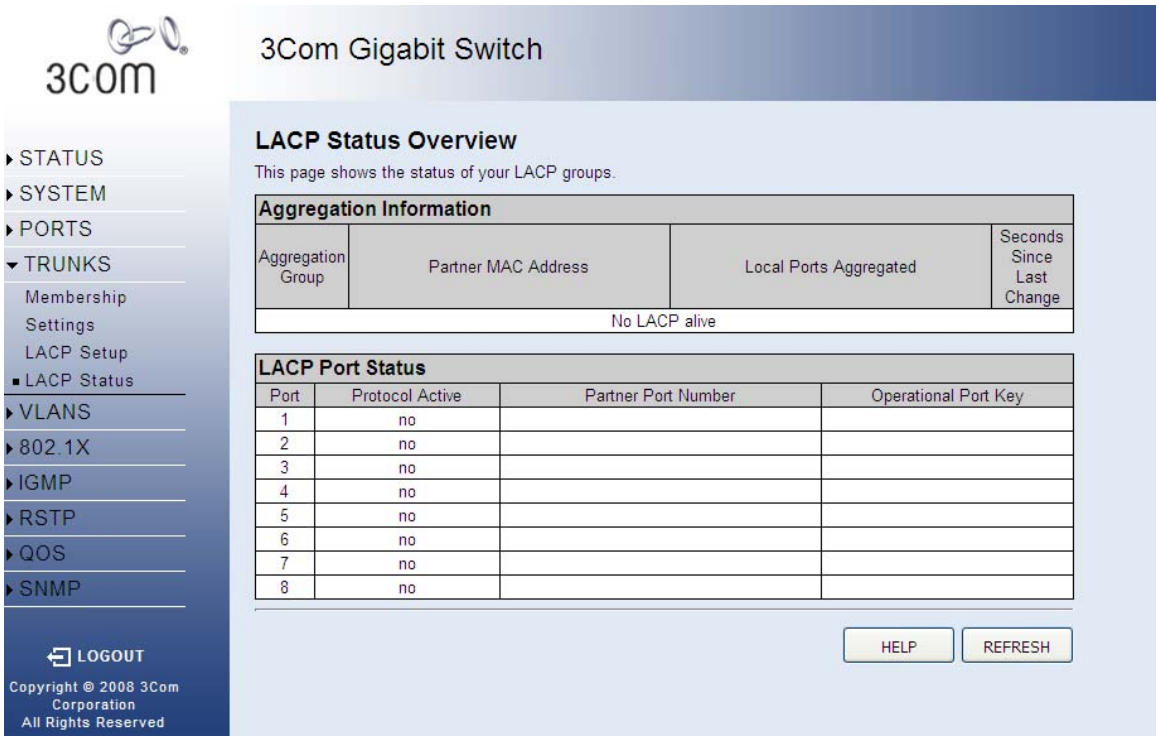
The columns are:

- **Port** - The front-panel port number.
- **LACP Enabled on Port** - Allows LACP to be enabled or disabled. When the box is checked, LACP is enabled.
- **Key Value (0..255, 0 means auto-generated key)** - Used to determine the link aggregation group membership, and to identify this device to other switches during negotiations.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **REFRESH** - Reloads the current page with the latest configuration settings.

6.4 LACP Status



This page displays the status of the LACP groups.

The LACP Aggregation table has one row for each LACP group. Normal means no LACP group is active. For active LACP groups, a new row is created from which the status of its port members are displayed. Status of each port is indicated by a colored box, which use color and number to differentiate status. There are two different tables on this page:

- **Aggregation Information** - Information on the Link Aggregation Groups.
- **LACP Port Status** - Information includes Protocol Active, Partner Port Number, and Operational Port Key

There are two main buttons associated with this page:

- **HELP** - Displays this text.
- **REFRESH** - Reloads the current page with the latest configuration settings.

6.4.1 Aggregation Information

The following information is displayed for Link Aggregation Groups:

- **Aggregation Group** - Displays the ID number of the LACP group.
- **Partner MAC Address** - Displays the MAC address of a device in the LACP group that is attached to this switch.
- **Local Port Aggregated** - Displays port member list of the local LACP group. The port members are ports on this switch.

- **Seconds Since Last Changed** - Number of seconds since the last LACP was received.

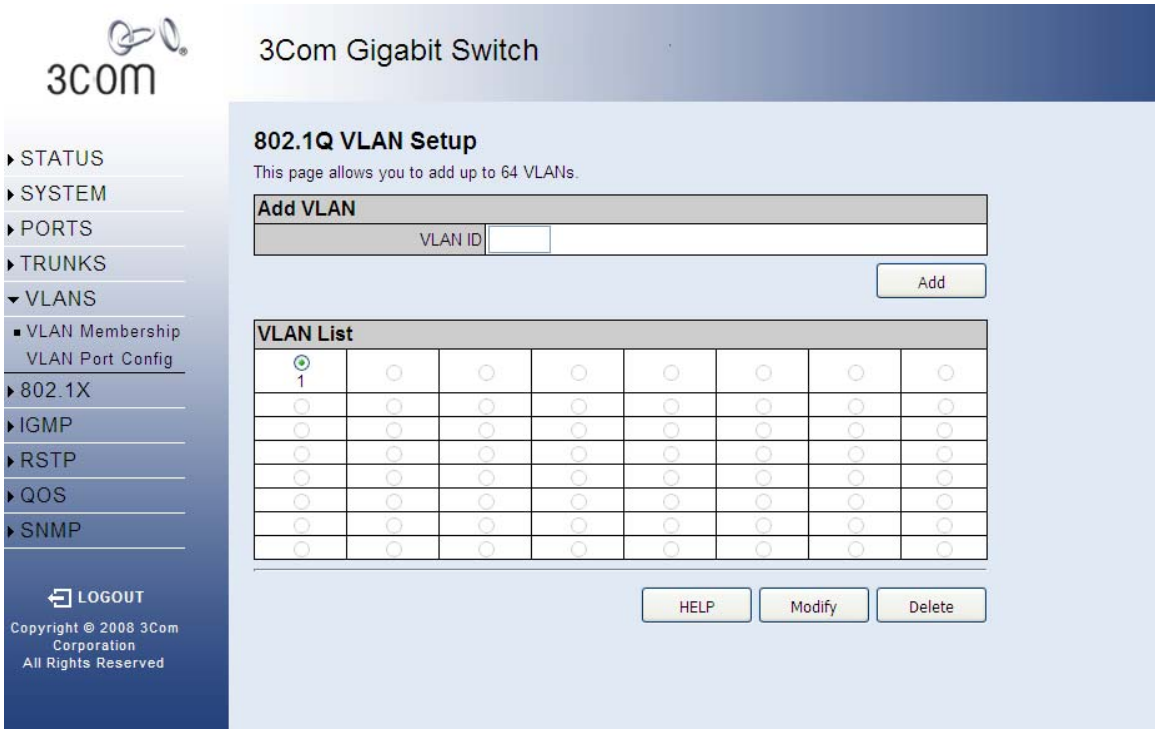
6.4.2 LACP Port Status

The following information is displayed for LACP port status:

- **Port** - Displays the ID number of the LACP group.
- **Protocol Active** - Shows if the port is a member of the active LACP group.
- **Partner Port Number** - The port number on the device in the LACP group that is attached to this port.
- **Operation Port Key** - The current operational value of the key for the LACP group.

7 VLANS

7.1 VLAN Membership



This page allows you to create up to 64 VLANs. You can also delete the VLANs or make changes to the VLAN membership and behavior of individual ports. VLANs are powerful but can be difficult to set up properly. If you are unfamiliar with VLANs please see the **Introduction to VLANs**. To create a VLAN, enter a VLAN ID into the VLAN ID field. After clicking the ADD button, you will be directed to the **802.1Q VLAN Group** page to add port members to the VLAN. Each row of the table corresponds to one VLAN.

There are four main buttons associated with this page:

- **HELP** - Displays this text.
- **ADD** - Creates a VLAN with the inputted VLAN ID.
- **MODIFY** - Choose a VLAN to modify.
- **DELETE** - Delete a VLAN from the VLAN table.

7.1.1 Introduction to VLANs

VLANs (or Virtual LANs) are logical partitions of the physical LAN. You can use VLANs to:

- Increase network performance
- Increase internal network security
- Create separate broadcast domains

If the network has adequate performance and security for your current needs, it is recommended that you leave the VLAN settings in the default configuration. The default configuration is as follows:

- All ports are members of VLAN 1
- The switch management interface is on VLAN 1 (this cannot be changed)
- All ports have a Port VLAN ID (PVID) of 1
- All ports can send and receive both VLAN-tagged and untagged packets (i.e. they are "hybrid" ports)

In the default configuration, any port is able to send traffic to any other port and a PC connected to any port will be able to reach the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.

There are three different parameters that can be configured for each port on the switch; **VLAN IDs** (VLAN membership), **PVID** and **Packet Type**. Note that the ports within a Trunk cannot be configured individually; configure the Trunk instead (Trunks are labeled T1 to T4).

7.1.2 VLAN IDs

- VLAN 1 is a special VLAN; it cannot be deleted and, if there is a possibility that a port could become isolated, the Web User-interface will add the port to VLAN 1.
- You can add up to 64 VLANs to the configuration of the switch. Each VLAN must be given a VLAN ID in the range 1-4094.
- A port can be a member of up to 64 VLANs.
- All packets travelling through the switch are associated with one and only one VLAN.
- If a port is not a member of a VLAN, it cannot send or receive packets associated with that VLAN.
- A tagged packet carries its VLAN ID in the payload of the packet.
- An untagged packet, received on a port with Packet Type set to All, is associated with the VLAN identified by the PVID.

7.1.3 PVID

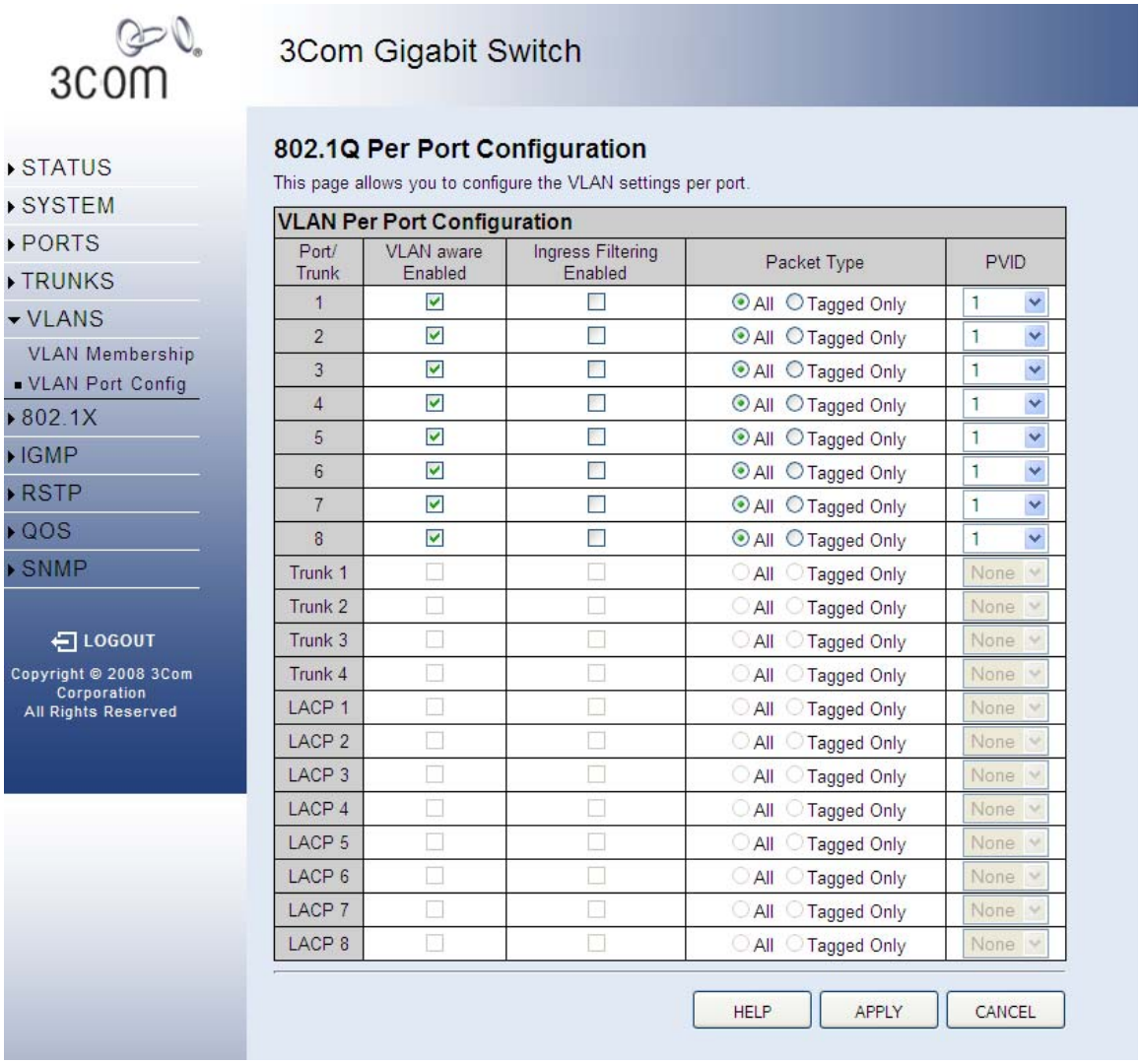
- The PVID is (Port VLAN ID) is the VLAN ID that is associated with untagged, ingress packets.
- It is not possible to remove a port from VLAN 1 unless its PVID has been changed to something other than 1.
- Outgoing packets are tagged unless the packet's VLAN ID is the same as the PVID. When the PVID is set to "None," all outgoing pacekts are tagged.

7.1.4 Packet Type

- PCs should be connected to ports with Packet Type set to All. PCs cannot, in general, send or receive tagged packets.
- Switches should be connected to each other with Packet Type set to Tagged.
- If the Packet Type is set to All, the port can accept incoming tagged and untagged packets. Untagged packets will be associated with the VLAN identified by the PVID. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. Outgoing packets will be tagged unless the packet's VLAN ID is the same as the PVID.

- If the Packet Type is set to Tagged, the port will drop untagged packets and will only send and receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. The PVID has no effect in this case.

7.2 VLAN Port Config



This page allows you to configure the VLAN parameters for individual ports. VLANs are powerful but can be difficult to set up properly. If you are unfamiliar with VLANs please see the **Introduction to VLANs**. Each row of the table corresponds to one port *or trunk*; trunked ports cannot be configured individually. The columns of the table are used as follows:

- **Port/Trunk** - The front-panel port number or the ID of a trunk.
- **VLAN Aware Enabled** - VLAN aware ports are able to use VLAN tagged frames to determine the destination of the frame. Click to enable or disable VLAN awareness mode for this port. (Default: Enabled)
- **Ingress Filtering Enabled** - If enabled, incoming frames for VLANs which do not include this ingress port as a member will be discarded. (Default: Disabled)

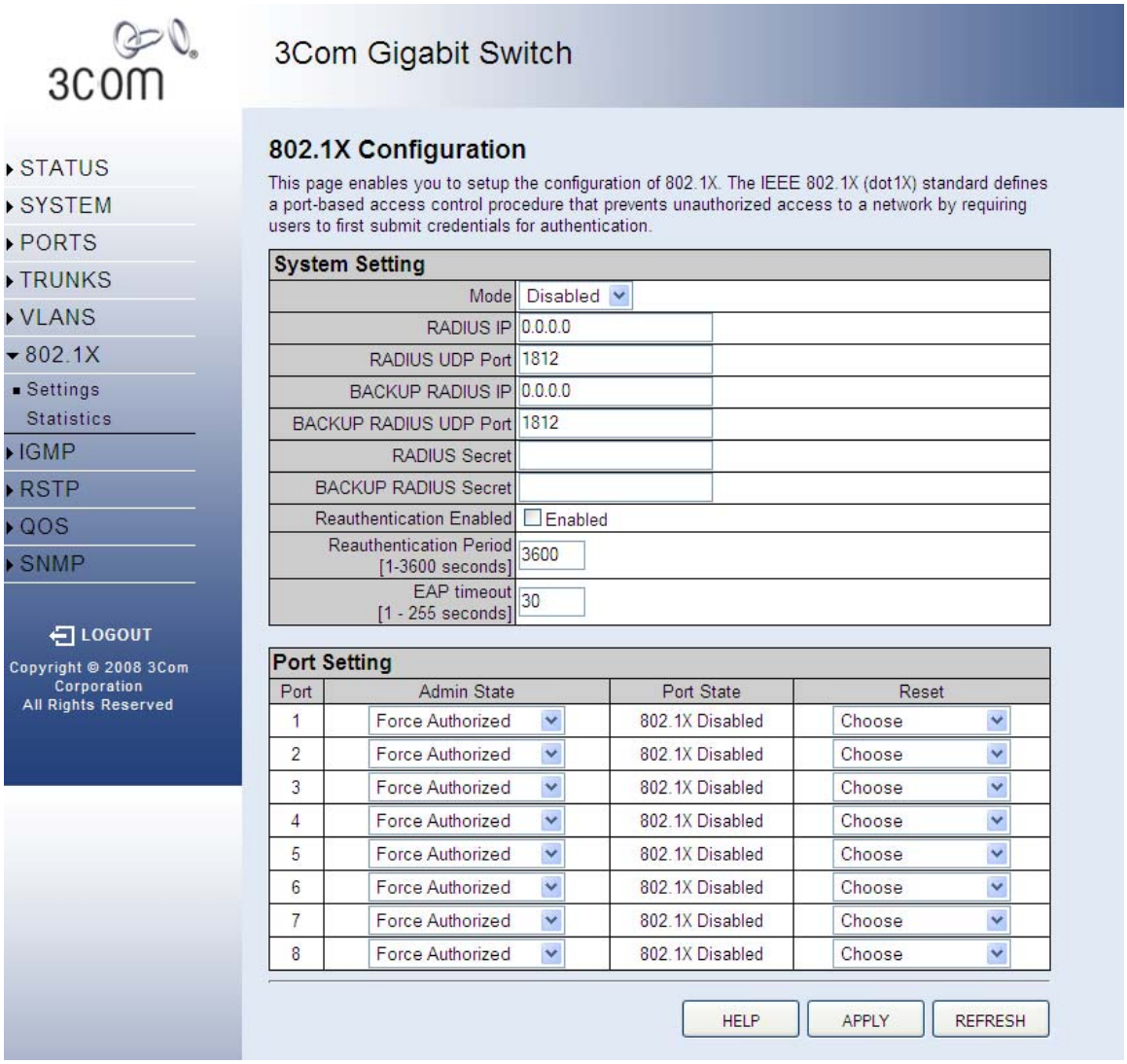
- **PVID** - Set the Port VLAN ID. (Default: All)
- **Packet Type** - Set a port's handling of tagged and untagged packets. (Default: 1)

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Saves the settings to memory, and updates the configuration. No changes are made to the switch's configuration until this button is pressed.
- **REFRESH** - Reloads the current page with the latest configuration setting.

8 802.1X

8.1 Settings



Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data. With IEEE 802.1X (802.1X), access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.

- **REFRESH** - Resends the information.

8.1.1 802.1x Settings

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

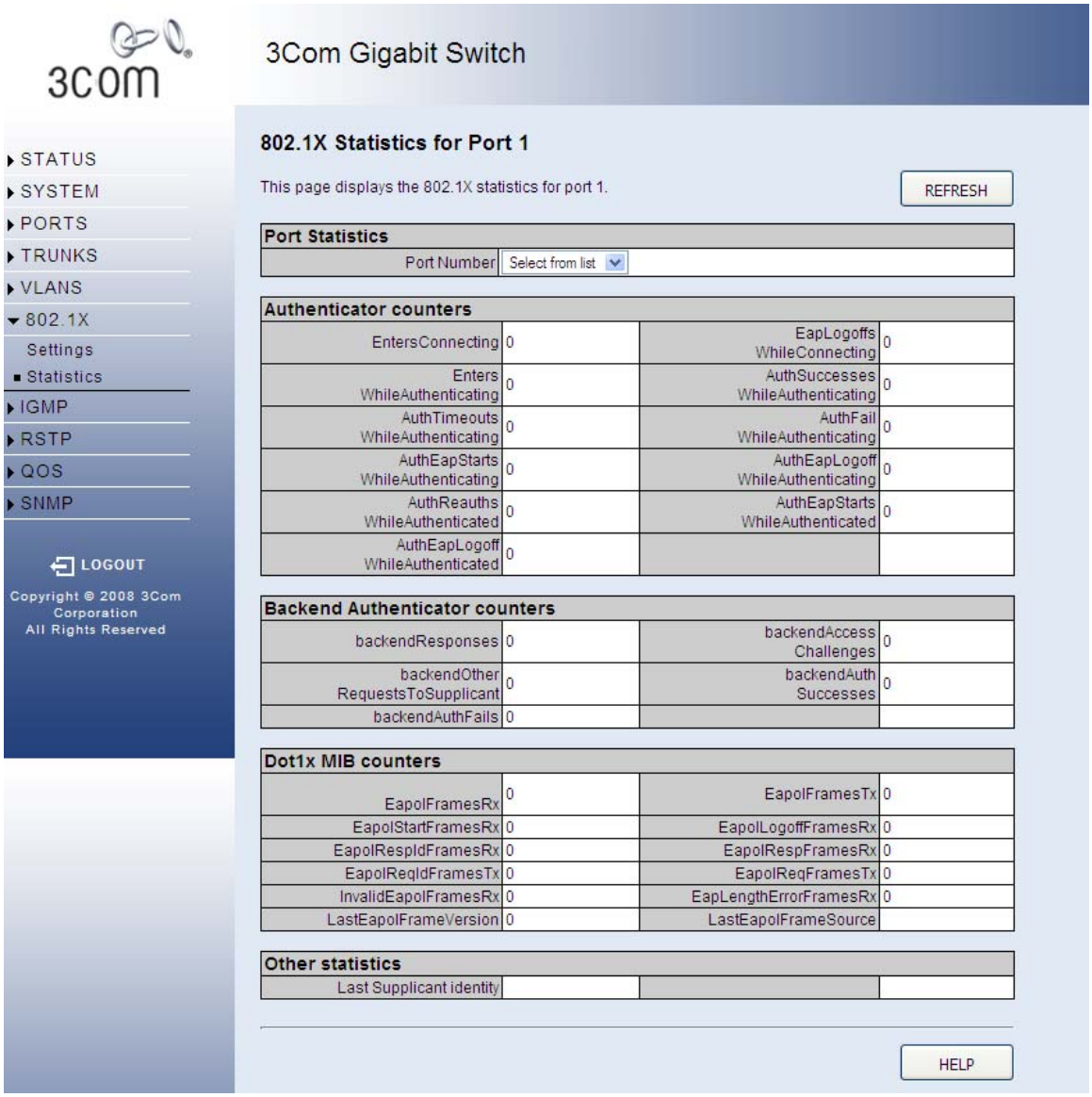
System Setting

- Mode - Indicates if 802.1X protocol is globally enabled or disabled on the switch.
- RADIUS IP - Sets the RADIUS server IP address.
- RADIUS UDP Port - Sets the UDP port to the use for the external RADIUS server.
- RADIUS Secret - Sets the text string used for encryption between the switch and the RADIUS server.
- Reauthentication Enabled - Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port.
- Reauthentication Period - Sets the time period after which a connected client must be re-authenticated.
- EAP timeout - The time the switch shall wait for the supplicant response before re-transmitting a packet.

Port Setting

- Port - The port number.
- Admin State - Sets the authentication mode to one of the following options:
    - Auto - Requires a 802.1X-aware client to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.
    - Force-Authorized - Forces the port to grant access to all clients, either 802.1X-aware or otherwise.
    - Force-Unauthorized - Forces the port to deny access to all clients, either 802.1X-aware or otherwise.
- Port State - The state of the port.
- Reset - Two options available:
    - Re-Authenticate - Schedules a reauthentication to whenever the quiet-period of the port runs out.
    - Force-Reinitialize - Bypasses the quiet-period of the port and enables immediate reauthentication regardless of the status for the quiet-period.

8.2 Statistics



Displays 802.1X statistics

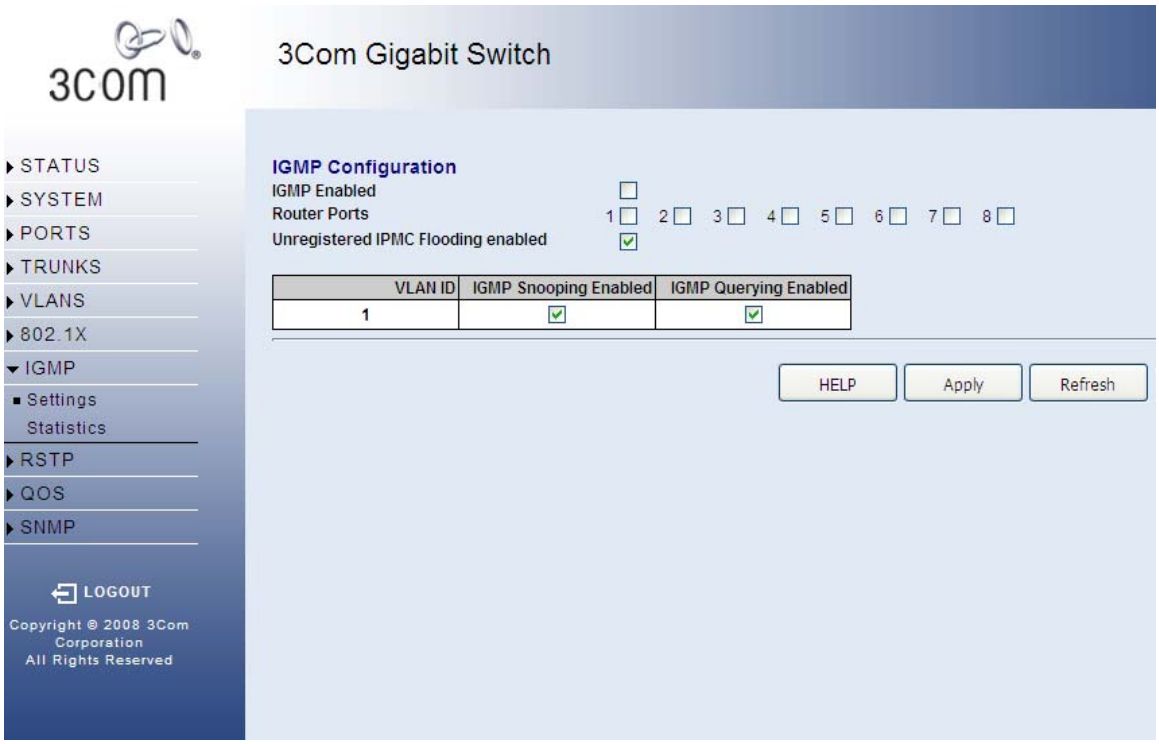
- Port Statistics - Statistics can be viewed on a per-port basis. Select the port that you want to view here.
- Authenticator counters - General statistics for authenticator.
- Backend Authenticator counters - General statistics for RADIUS server.
- 802.1X MIB counters - MIB module defined for 802.1X.

There are two main buttons associated with this page:

- **HELP** - Displays this text.
- **REFRESH** - Resends the information.

9 IGMP SNOOPING

9.1 IGMP Settings



This page enables customers to setup the configuration of IGMPSNOOP. IGMPSNOOP monitors IGMP service requests passing between multicast clients and servers, and dynamically configures the ports which need to receive the mulitcast traffic. For IGMPV3, basic support for reports only, Source Multicast not supported.. The page is composed of two tables:

- **IGMP Snooping Configuration** - Configure global system settings.
- **IGMP Snooping VLAN Configuration** - Configure VLAN related settings.

There are three main buttons associated with this page:

- **HELP** - Displays this text.
- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **REFRESH** - Reloads the current page with the latest configuration settings.

9.1.1 IGMP Snooping Configuration

There are three configurable parameters in this table. As follows:

- **IGMP Enabled** - When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

- **Router Ports** - Set if ports are conneting to the IGMP administrative routers.
- **Unregistered IPMC Flooding enabled** - Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.

If the network has adequate performance and security for your current needs, it is recommended that you leave the VLAN settings in the default configuration. The default configuration is as follows:

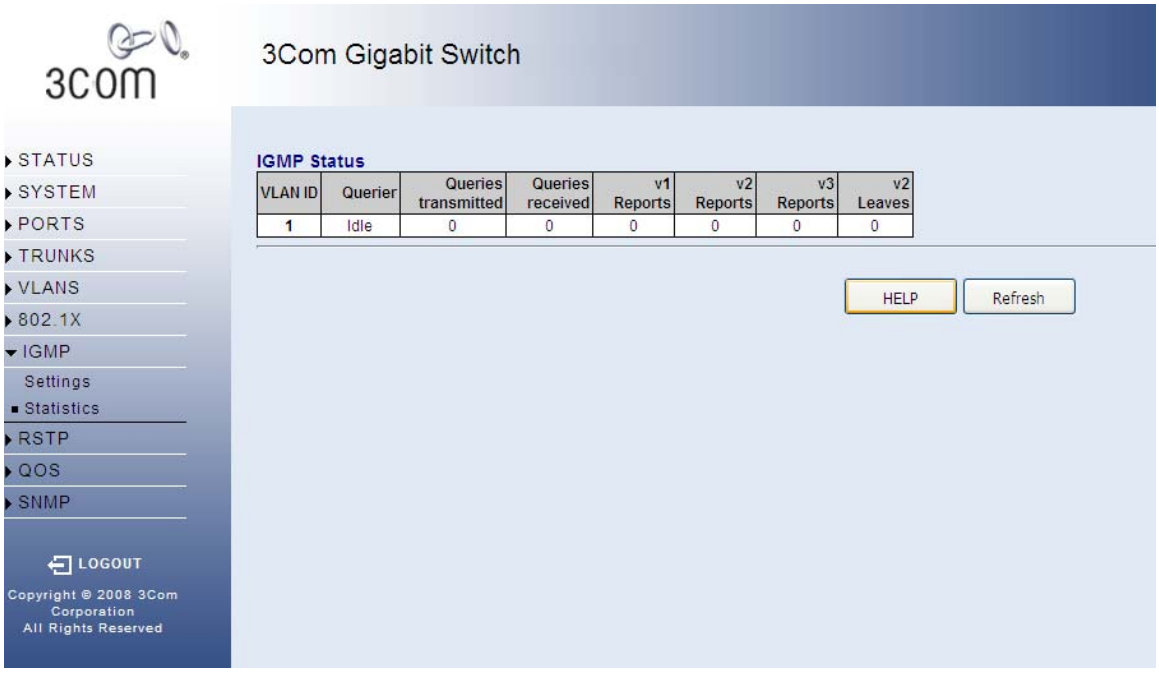
- All ports are members of VLAN 1
- The switch management interface is on VLAN 1 (this cannot be changed)
- All ports have a Port VLAN ID (PVID) of 1
- All ports can send and receive both VLAN-tagged and untagged packets (i.e. they are "hybrid" ports)

9.1.2 IGMP VLAN Configuration

The table has one row for each port and four columns. The columns are:

- **VLAN ID** - The VLAN ID. It can not be changed.
- **IGMP Snooping Enabled** -When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.
- **IGMP Querying Enabled** - When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

9.2 IGMP Snoop Status



This page shows IGMPSNOOP instances and port states. There is one tables on this page:

- **IGMPSNOOP Status** - Show the IGMPSNOOP statistics for the whole switch.

There are three main buttons associated with this page:

- **HELP** - Displays this window.
- **REFRESH** - Refreshes the page with the current status

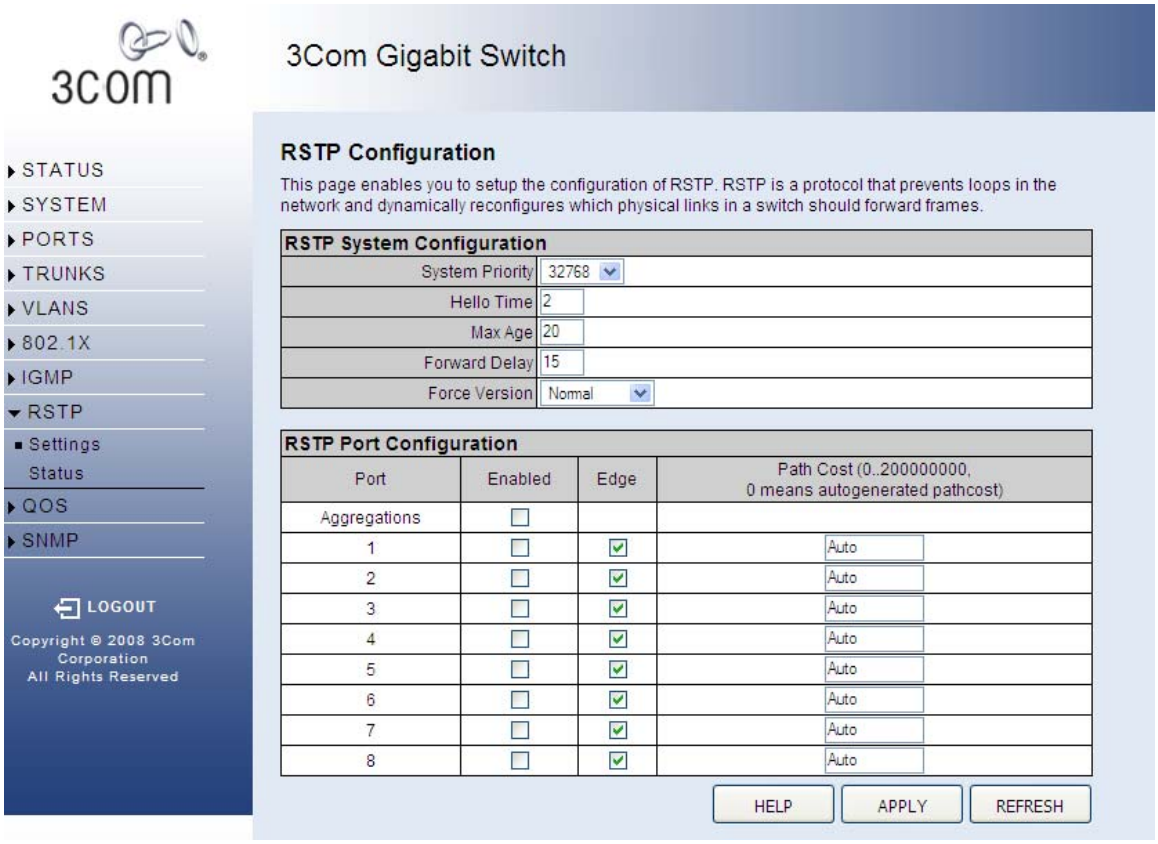
9.2.1 IGMP Snoop Statistics

The table has one row for each port and seven columns. The columns are:

- **VLAN ID** - VLAN ID number.
- **Querier** - Show whether Querying is enabled.
- **Queries transmitted** - Show the number of transmitted Query packets.
- **Queries received** - Show the number of received Query packets.
- **v1 Reports** - Show the number of received v1 Report packets.
- **v2 Reports** - Show the number of received v2 Report packets.
- **v3 Reports** - Show the number of received v2 Report packets.
- **v3 Leave** - Show the number of v3 leave packets received.

10 RSTP

10.1 RSTP System Configuration



This page enables you to setup the configuration of RSTP. **RSTP** is a protocol that prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames. The page is composed of two tables:

- **RSTP System Configuration** - Configure global system settings.
- **RSTP Port Configuration** - Setup port related settings.

There are three main buttons associated with this page:

- **HELP** - Displays this window.
- **APPLY** - Updates the Switch configuration. No changes are made to the configuration until this button is pressed.
- **REFRESH** - Refreshes the page with the current RSTP configuration.

Spanning Tree Introduction

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which

automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

10.1.1 RSTP System Configuration

There are five configurable parameters in this table. As follows:

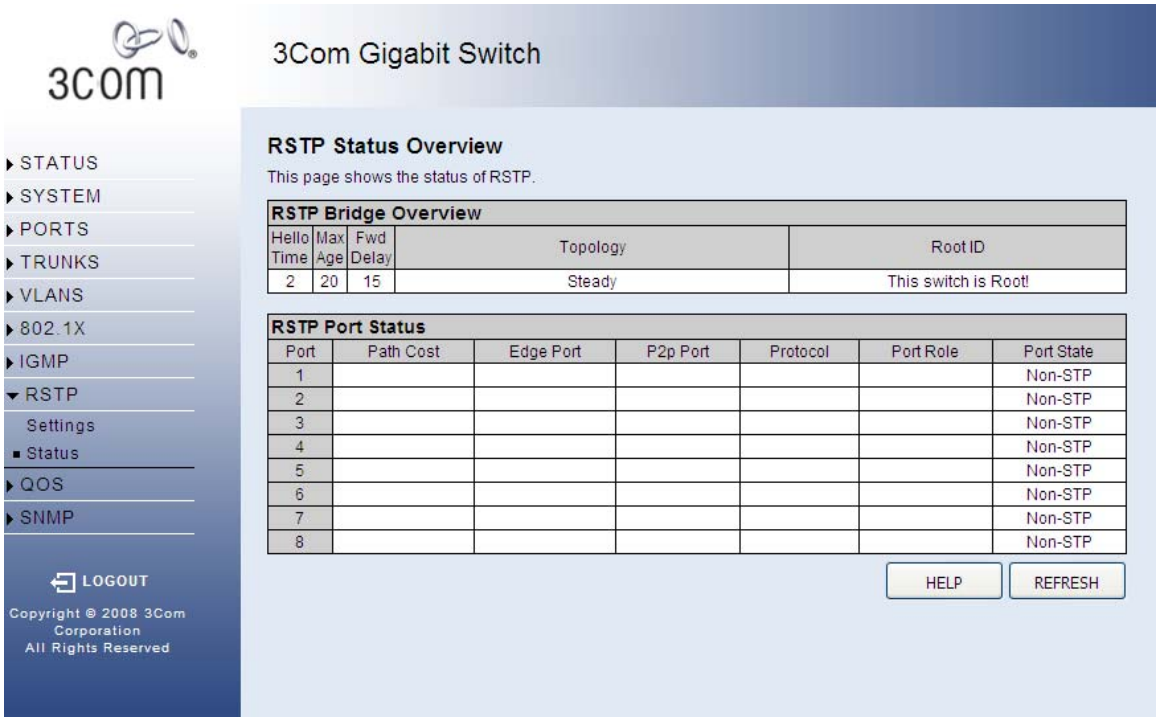
- **System Priority** - This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 16 distinct values.
- **Hello Time** - Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1 - 10 (default is 2).
- **Max Age** - The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6 - 40 (default is 20).
- **Forward Delay** - ?The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 - 30 (default is 15).
- **Force Version** - Set and show the RSTP protocol to use. Normal - use RSTP, Compatible - compatible with STP.

10.1.2 RSTP System Configuration

The table has one row for each port and four columns. The columns are:

- **Port** - The port ID. It can not be changed. Aggregations means any configured trunk group.
- **Enabled** - Click on the tick-box to enable/disable the RSTP protocol for the port.
- **Edge** - Expect the port to be an edge port (linking to an end station) or a link to another STP device.
- **Path Cost** - This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP pathcost on the port. Number between 0 - 200000000. 0 means autogenerated pathcost.

10.2 RSTP Status



This page shows RSTP bridge and port states. There are two tables on this page:

- **RSTP Bridge Overview** - Show the RSTP settings for the whole switch.
- **RSTP Port Status** - Detailed RSTP information for each port.

There are two main buttons associated with this page:

- **HELP** - Displays this window.
- **REFRESH** - Refreshes the page with the current status.

10.2.1 RSTP Bridge Overview

The **RSTP Bridge Overview** table has one row to display settings for the whole switch. Hello Time, Maximum Age and Forward Delay are displayed. Topology shows the switch current state. Root ID indicates the root port ID for the switch.

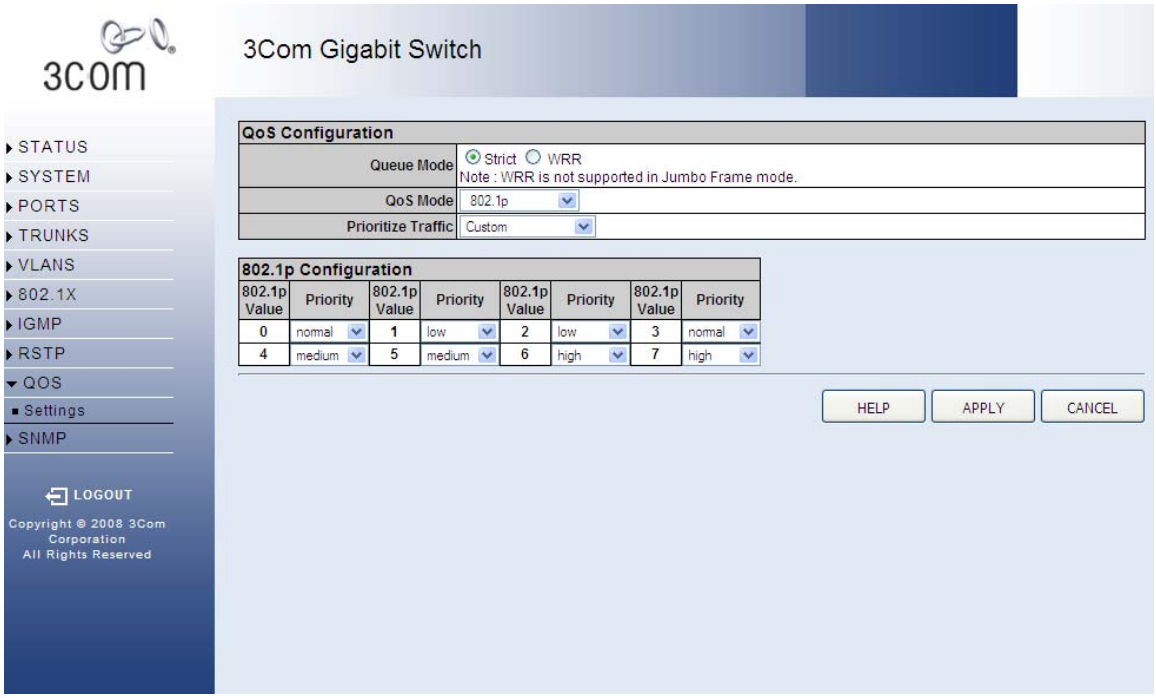
10.2.2 RSTP Port Status

The table has one row for each port and seven columns. The columns are:

- **Port/Trunk** - Port/Trunk ID number.
- **VLAN ID** - VLAN IDs of the port.
- **Path Cost** - Show the path cost on this port.
- **Edge Port** - Yes if the port is an edge port which connects to an end station.
- **P2p Port** - Yes if the port link is connected to another STP device.
- **Protocol** - Show the running protocol, RSTP or STP.

- **Port State** - Show the current port state, blocking, forwarding, learning etc.

11 QoS



11.1 QoS Configuration

QoS (Quality of Service) is a mechanism which is used to prioritize certain traffic as it is moves through the switch. Traffic can be classified as High, Medium, Normal or Low priority. This switch features both strict priority-based and weighted round-robin (WRR) forwarding, with guaranteed bandwidth allocation for the different QOS classes. The queueing method can be selected using the **Queue Mode** drop-down list:

- **Strict priority** - Higher priority frames take precedence over lower priority frames during forwarding. In case of congestion, the lowest priority traffic is dropped before higher priority frames. Head-of-queue blocking maybe encountered by using this mode.
- **WRR** - In this mode, all priorities can be guaranteed a share of the bandwidth when the system is overloaded. The bandwidth sharing percentage can be adjusted by specifying the four QOS class with different ratio in **WRR Weight**, which appears after **WRR** is enabled in **Queue Mode**.

Note: WRR is selectable when **Jumbo Frame** is disabled in **Ports > Settings**.

You can select how traffic is prioritized by using one of the three QoS modes which is selected using the **QoS Mode** drop-down list:

- **QoS Disabled** - QoS is turned off and all packets have equal priority.
- **802.1p** - Packets are prioritzed using the content of the VLAN-tag.
- **DSCP** - Packets are prioritized using the DSCP (Differentiated Services Code Point) value.

Note: Only one QoS mode can be active at one time. It is not possible, for example, to prioritise traffic using the DSCP *and* 802.1p

There are three main buttons associated with this page:

- **HELP** - Displays this window.
- **APPLY** - Saves the settings to memory, and updates the configuration. No changes are made to the switch's configuration until this button is pressed.
- **REFRESH** - Reloads the current page with the latest configuration setting.

11.1.1 802.1p

The 802.1p field is held within the VLAN-tag of a packet. The field is three bits long so can hold eight values; 0 - 7 inclusive. When **QoS Mode** is set to **802.1p**, the **802.1p Configuration** table appears which allows a priority to be set for each of the eight values.

You can use the **Prioritize Traffic** drop-down list to quickly set the values in the **802.1p Configuration** table. Select **All Low Priority** to set all values to **low** priority, **All Normal Priority** to set all values to **normal** priority, **All Medium Priority** to set all values to **medium** priority, or select **All High Priority** to set all values to **high** priority. Use **Custom** if you want to set each value individually.

Note: Because end-stations, like PCs, are not usually VLAN aware, they do not create VLAN-tagged frames. As a result, this method of prioritization is not ideal when there are a lot of PCs connected to the Switch.

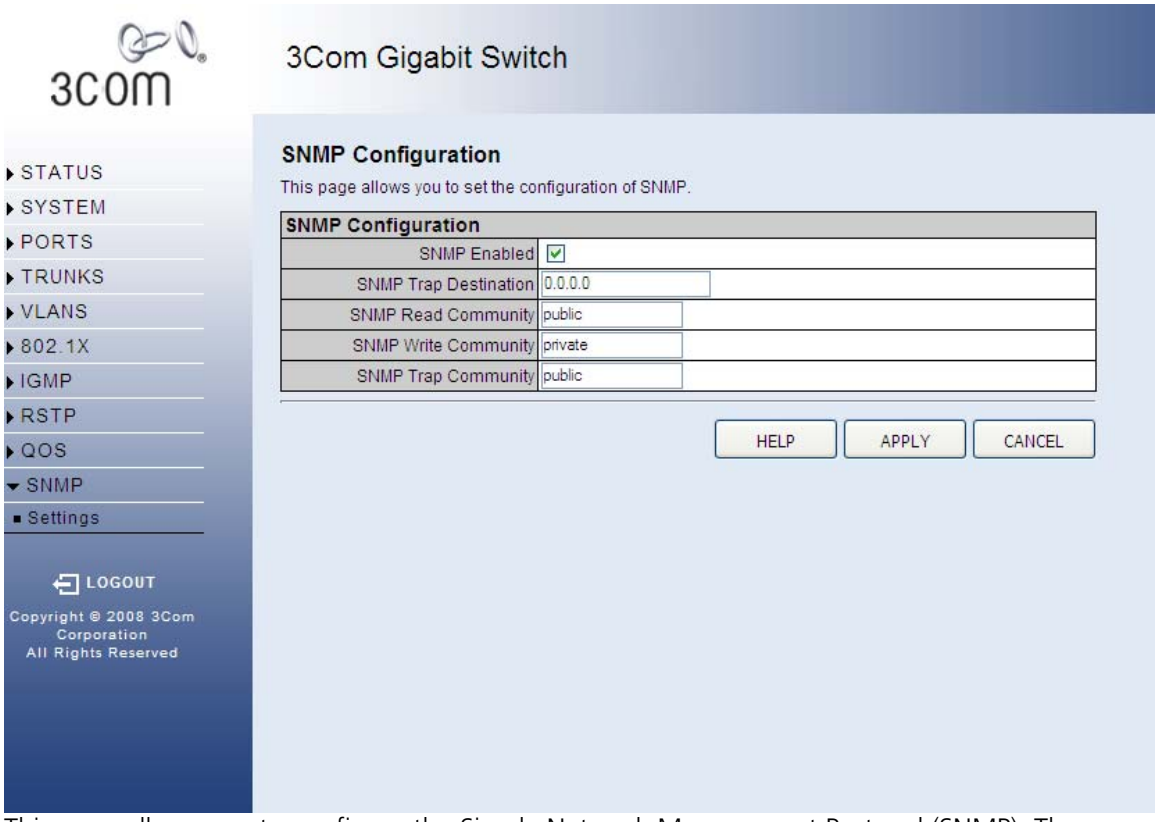
11.1.2 DSCP

The Differentiated Services Code Point (DSCP) is a six bit field that is contained within an IP (TCP or UDP) header. Six bits allows the DSCP field to take any value in the range 0 - 63 inclusive. When **QoS Mode** is set to **DSCP**, the **DSCP Configuration** table appears which allows a priority to be set for each of the DSCP values.

You can use the **Prioritize Traffic** drop-down list to quickly set the values in the **DSCP Configuration** table. Select **All Low Priority** to set all values to **low** priority, **All Normal Priority** to set all values to **normal** priority, **All Medium Priority** to set all values to **medium** priority, or select **All High Priority** to set all values to **high** priority. Use **Custom** if you want to set each value individually.

12 SNMP

12.1 Settings



This page allows you to configure the Simple Network Management Protocol (SNMP). The SNMP agent permits the switch to be managed from any system in the network using management software. You can set the following options:

- **SNMP Enabled** -Activate or deactivate SNMP.
- **SNMP Trap Destination** - IP address of the trap manager.
  Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station. SNMP trap destination specifies the IP address of the trap manager.
- **SNMP Read Community** - A community string that acts like a password and permits access to the SNMP protocol. The read community string specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **SNMP Write Community** - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
- **SNMP Trap Community** - Community string sent with the notification operation.

There are three main buttons associated with this page:

- **HELP** - Displays this text.

- **APPLY** - Updates the switch configuration. No changes are made to the configuration until this button is pressed.
- **CANCEL** - All changes made to the page are discarded and the switch configuration remains unchanged.

13 3COM NETWORK MANAGEMENT

3Com has a range of network management applications to address networks of all sizes and complexity, from small and medium businesses through large enterprises. The applications include:

- 3Com Network Supervisor
- 3Com Network Director
- 3Com Network Access Manager
- 3Com Enterprise Management Suite
- Integration Kit with HP OpenView Network Node Manager

Details of these and other 3Com Network Management Solutions can be found at www.3com.com/network_management

3Com Network Supervisor

3Com® Network Supervisor (3NS) is an easy-to-use management application that graphically discovers, maps, and monitors the network and links. It maps devices and connections so you can easily:

- Monitor stress levels
- Set thresholds and alerts
- View network events
- Generate reports in user-defined formats
- Launch embedded device configuration tools

3NS is configured with intelligent defaults and the ability to detect network misconfigurations. It can also offer optimization suggestions, making this application ideal for network managers with all levels of experience.

To find out more about 3Com Network Supervisor and to download a trial version, go to: www.3com.com/3ns

3Com Network Director

3Com Network Director (3ND) is a standalone application that allows you to carry out key management and administrative tasks on midsized networks. By using 3ND you can discover,

map, and monitor all your 3Com devices on the network. It simplifies tasks such as backup and restore for 3Com device configurations as well as firmware and agent upgrades. 3ND makes it easy to roll out network-wide configuration changes with its intelligent VLAN configuration tools and the powerful template based configuration tools. Detailed statistical monitoring and historical reporting give you visibility into how your network is performing.

To find out more about how 3Com Network Director can help you manage your 3Com network and to download a trial version, go to: www.3com.com/3nd

3Com Network Access Manager

3Com Network Access Manager is installed seamlessly into Microsoft Active Directory and Internet Authentication Service (IAS). It simplifies the task of securing the network perimeter by allowing the administrator to easily control network access directly from the "Users and Computers" console in Microsoft Active Directory. With a single click, a user (or even an entire department) can be moved to a different VLAN, or a computer can be blocked from connecting to the network.

3Com Network Access Manager leverages the advanced desktop security capabilities of 3Com switches and wireless access points (using IEEE 802.1X or RADA desktop authentication) to control both user and computer access to the network.

To find out more about 3Com Network Access Manager, go to: www.3com.com/NAM

3Com Enterprise Management Suite

3Com Enterprise Management Suite (EMS) delivers comprehensive management that is flexible and scalable enough to meet the needs of the largest enterprises and advanced networks.

This solution provides particularly powerful configuration and change control functionalities, including the capability to:

- Customize scheduled bulk operations
- Create a detailed audit trail of all network changes
- Support multiple distributed IT users with varying access levels and individualized network resource control

The client-server offering operates on Windows and UNIX (Linux and Solaris) systems.

3Com EMS is available in four packages, varying in the maximum number of devices actively managed. These include SNMP-capable devices such as switches, routers, security switches, the 3Com VCX™ IP Telephony server, and wireless access points:

- Up to 250 devices
- Up to 1,000 devices
- Up to 5,000 devices
- An unlimited number of devices

To find out more about 3Com Enterprise Management Suite, go to: www.3com.com/ems

Integration Kit with HP OpenView Network Node Manager

3Com Integration Kit for HP OpenView Network Node Manager offers businesses the option of managing their 3Com network directly from HP OpenView Network Node Manager. The kit includes Object IDs, icons, MIBs, and traps for 3Com devices. The package supports both Windows platforms and UNIX or Solaris platforms. It can be installed as a standalone plug-in to HP OpenView, or used with a 3Com management application such as 3Com Enterprise Management Suite (EMS).

To find out more about 3Com Integration Kit for HP OpenView Network Node Manager, go to: www.3com.com/hpovintkit

14 DEVICE SPECIFICATIONS AND FEATURES

Related Standards

The 3Com® OfficeConnect Managed Gigabit Switch has been designed to the following standards:

Function	8802-3, IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab (Gigabit Ethernet), IEEE 802.1D (Bridging)
Safety	UL 60950-1, EN 60950-1, CSA 22.2 No. 60950-1, IEC 60950-1
EMC Emissions	EN55022 Class A, AS/NZS CISPR 22 Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, EN61000-3-2, EN61000-3-3, ICES-003 Class A
EMC Immunity	EN55024

Environmental

Operating Temperature	0 to 40 °C (32 to 104°F).
Storage Temperature	–40 to +70 °C (–40 to +158 °F)
Humidity	0-95% (non-condensing)
Standard	EN 60068 (IEC 68)

Physical

Width	330 mm (12.99 in.)
Depth	203.2 mm (8 in.)
Height	44 mm (1.73 in.) or ½ U.
Weight	2.23 kg (4.91 lb)
Mounting	Standalone or wall mounting

Electrical

Input Voltage	12V DC
Current Rating	1 Amp (Max)
Maximum Power Consumption	23.9 BTU/hr (7.6 Watts)
Max Heat Dissipation	19 BTU/hr

Switch Features

This section describes the device features. The system supports the following features:

Table 6 Features of the OfficeConnect Managed Gigabit Switch

Feature	Description
Auto Negotiation	The purpose of auto negotiation is to allow a device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their abilities. Auto negotiation is performed totally within the physical layers during link initiation, without any additional overhead to either the MAC or higher protocol layers. Auto negotiation allows the ports to do the following: ▪ Advertise their abilities ▪ Acknowledge receipt and understanding of the common modes of operation that both devices share ▪ Reject the use of operational modes that are not shared by both devices ▪ Configure each port for the highest-level operational mode that both ports can support
Automatic MAC Addresses Aging	MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.
Back Pressure	On half duplex links, the receiver may employ back pressure (i.e. occupy the link so it is unavailable for additional traffic), to temporarily prevent the sender from transmitting additional traffic. This is used to prevent buffer overflows.
Address Resolution Protocol (ARP)	ARP converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.
Class Of Service (CoS)	Provide traffic belonging to a group preferential service (in terms of allocation of system resources), possibly at the expense of other traffic.

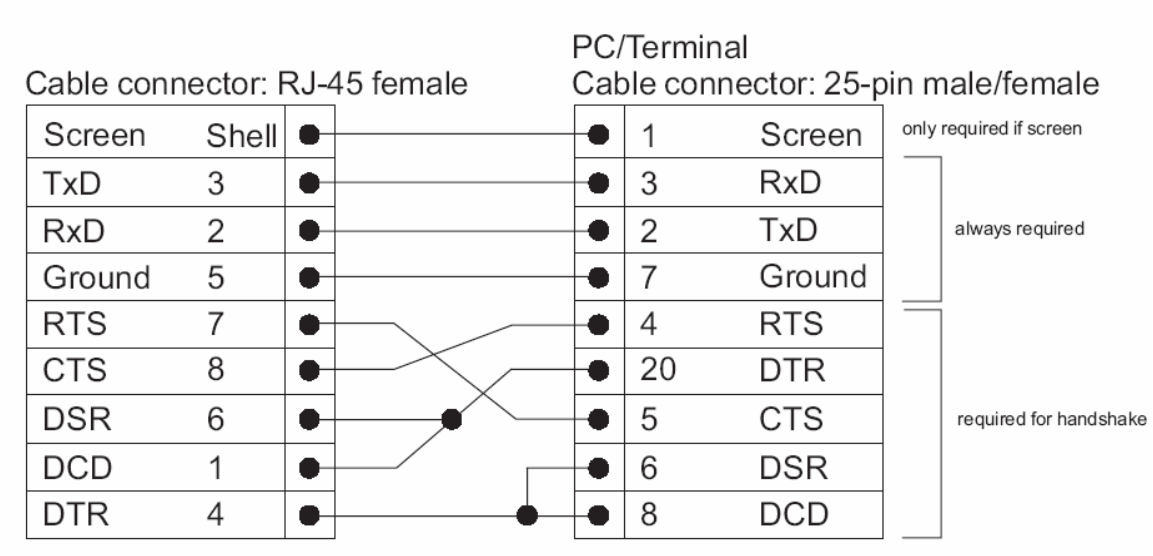
Feature	Description
Command Line Interface	The Command Line Interface (CLI) is an interface using a serial connection that allows basic features to be configured, including IP address management and firmware upgrading. The CLI is not intended as the main interface for the switch.
Configuration File Management	The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.
DHCP Clients	Dynamic Host Client Protocol. DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process.
Domain Name System	Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the name into a numeric IP address. For example, www.ipexample.com is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses.
Fast Link	STP can take up to 30-60 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies where forwarding loops do not occur.
Full 802.1Q VLAN Tagging Compliance	IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs and the protocols and algorithms involved in the provision of these services. An important requirement included in this standard is the ability to mark frames with a desired Class of Service (CoS) tag value.
IGMP Snooping	IGMP Snooping examines IGMP frame contents, when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames.
LACP	LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds and monitors the port binding within the system.
Link Aggregated Groups	The system provides up to four Link Aggregated Groups (LAGs). Aggregated Links may be defined, each with up to eight member ports, to form a single LAG. LAGs provide: ▪ Fault tolerance protection from physical link disruption ▪ Higher bandwidth connections ▪ Improved bandwidth granularity ▪ High bandwidth server connectivity ▪ LAG is composed of ports with the same speed, set to full-duplex operation.

MAC Address Capacity Support	The device supports up to 8K MAC addresses. The device reserves specific MAC addresses for system use.
MAC Multicast Support	Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 Multicast service is where a single frame is addressed to a specific Multicast address, from where copies of the frame are transmitted to the relevant ports.
MDI/MDIX Support	The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).
Password Management	Password management provides increased network security and improved password control. Passwords for HTTP, HTTPS, and SNMP access are assigned security features. For more information on Password Management, see "Default Users and Passwords" page 29.
Port-based Authentication	Port-based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).
Port-based Virtual LANs	Port-based VLANs classify incoming packets to VLANs based on their ingress port.
Port Mirroring	Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.
Power over Ethernet	Provides power to devices over LAN connection.
RADIUS Clients	RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information.
Rapid Spanning Tree	Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.
Remote Monitoring	Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.
Self-Learning MAC Addresses	The device enables automatic MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table
SNMP Alarms and Trap Logs	The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.

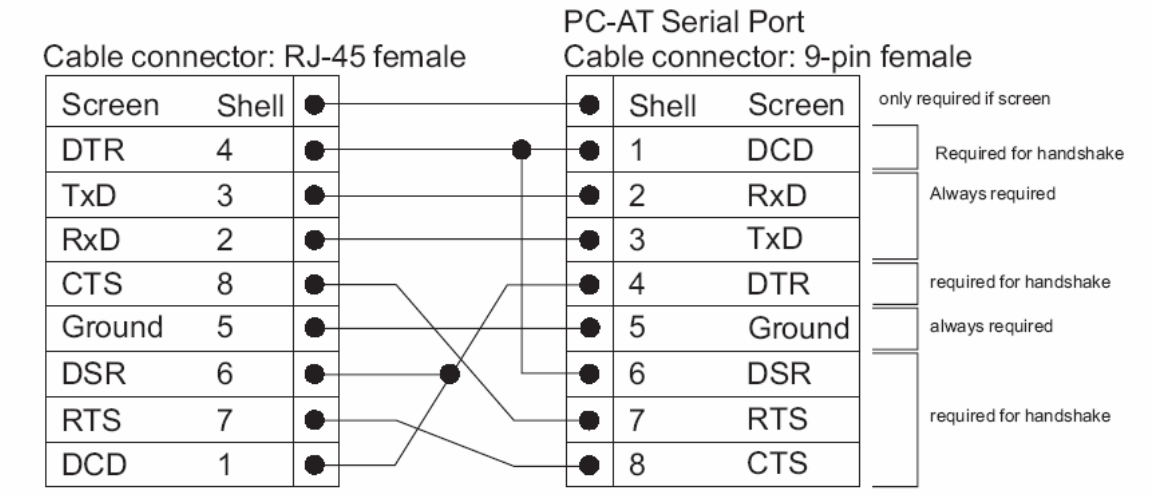
SNMP Versions 1 and 2	Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the system.
Spanning Tree Protocol	802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.
SSL	Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.
Static MAC Entries	MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user-defined entries are not subject to aging, and are preserved across resets and reboots.
TCP	Transport Control Protocol (TCP). TCP connections are defined between 2 ports by an initial synchronization exchange. TCP ports are identified by an IP address and a 16-bit port number. Octets streams are divided into TCP packets, each carrying a sequence number.
TFTP Trivial File Transfer Protocol	The device supports boot image, software and configuration upload/download via TFTP.
Virtual Cable Testing	VCT detects and reports copper link cabling occurrences, such as open cables and cable shorts.
VLAN Support	VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.
Web-based Management	With web-based management, the system can be managed from any web browser. The system contains a Web Server, which serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings.

15 PIN-OUTS

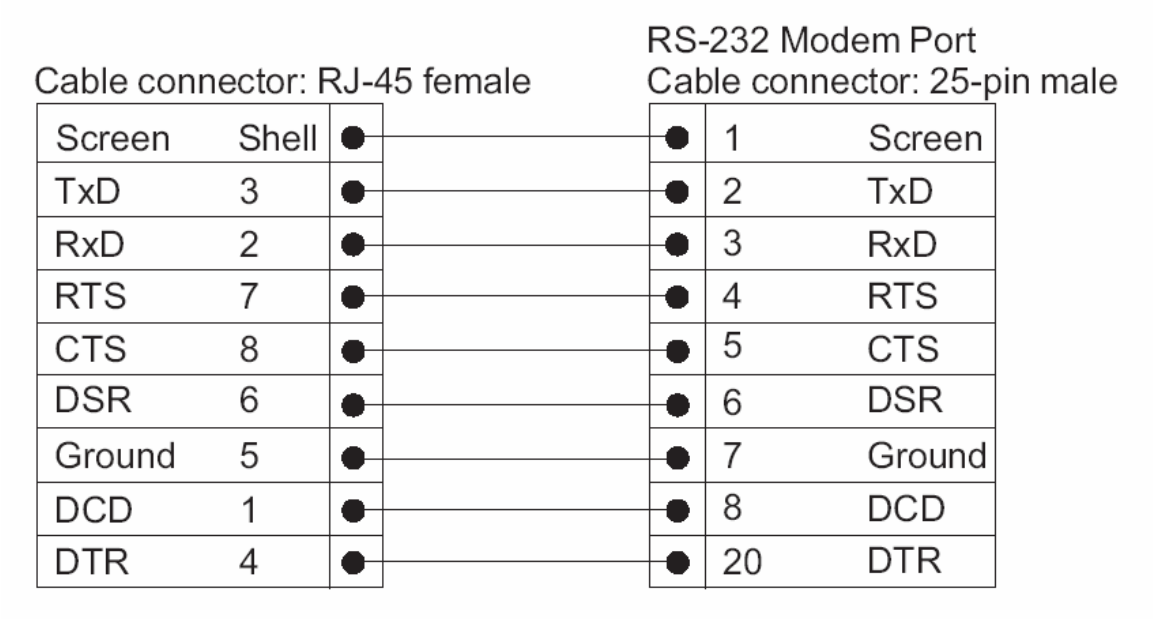
Null Modem Cable RJ-45 to RS-232 25-pin



PC-AT Cable RJ-45 to 9-pin



Modem Cable RJ-45 to RS-232 25-pin



Ethernet Port RJ-45 Pin Assignment 10/100 and 1000BASE-T RJ45 Connections

Table 7 Pin Assignments

Pin Number	10/100	1000
Ports configured as MDI		
1	Transmit Data +	Bidirectional Data A+
2	Transmit Data •	Bidirectional Data A•
3	Receive Data +	Bidirectional Data B+
4	Not assigned	Bidirectional Data C+
5	Not assigned	Bidirectional Data C•
6	Receive Data •	Bidirectional Data B•
7	Not assigned	Bidirectional Data D+
8	Not assigned	Bidirectional Data D•

Table 8 Pin Assignments

Pin Number	10/100	1000
Ports configured as MDIX		
1	Receive Data +	Bidirectional Data B+
2	Receive Data •	Bidirectional Data B•
3	Transmit Data +	Bidirectional Data A+
4	Not assigned	Bidirectional Data A•
5	Not assigned	Bidirectional Data D+
6	Transmit Data •	Bidirectional Data D•
7	Not assigned	Bidirectional Data C+
8	Not assigned	Bidirectional Data C•

16 3COM CLI REFERENCE GUIDE

This section describes using the *Command Line Interface*(CLI) to manage the device. The device is managed through the CLI from a direct connection to the device console port.

Getting Started with the Command Line Interface

Using the CLI, network managers enter configuration commands and parameters to configure the device. Using the CLI is very similar to entering commands on a UNIX system.

Console Port

To start using the CLI via a console port:

1. Connect the RJ-45 cable to the Console port of the switch to the serial port of the terminal or computer running the terminal emulation application.
2. Set the baud rate to 38400.
3. Set the data format to 8 data bits, 1 stop bit, and no parity.
4. Set Flow Control to **none**.
5. Under **Properties**, select **VT100** for **Emulation** mode.
6. Select T**erminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** (not **Windows keys**).

Logging on to the CLI

The Login process requires a User Name and Password. The default user name for first time configuration is **admin**. No password is required. User names and passwords are case sensitive.

To logon to the CLI Interface:

1. After the switch has booted up, The **Login** prompt displays:

```
Username:
```

2. Enter your **User Name** at the Login prompt.
3. Press **Enter**. The **Password** prompt displays:

```
Password:
```

The Login information is verified, and displays the following

```
Press ? or help to get help. The help depends on the context:
   - At top level, a list of command groups will be shown.
   - At group level, a list of the command syntaxes will be shown.
   - If given after a command, the syntax and a description of the
     command will be shown.
>
```

If the password if invalid, the following message appears and the Login process restarts:

```
Incorrect password
Username:
```

Concurrent CLI Sessions

The command line interface supports one CLI session.

Closing CLI Sessions

To logout of the CLI session, enter **`exit`** and press Return.

CLI Commands

This Command section contains the following commands:

- ?
- System Restore Default
- System Reboot
- Console Password
- IP Setup
- IP Status
- IP Ping
- IP Dhcp
- IP tftpget

The command section is divided into three sub-sections:

- System
- Console
- IP

You can navigate into each section by typing one of the above names. Each section has a number of sub commands. You can enter the full command from the top of the menu structure, for example **`IP Ping`**, or you can enter the IP sub-menu (by entering **`IP`** and pressing Return) and just type **`Ping`**. To move up from within a sub menu, enter **`up`** and press **`Return`**.

***Note**: the CLI commands are not case sensitive. You must enter the whole command.*

?

The **?** command displays a list of CLI commands. The list of commands shown depends on which sub-menu you are currently in. At the top level this command lists the sub-menus.

Syntax

?

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

The following displays the list presented for the **?** command:

```
>?
Commands at top level:
System      - System commands
Console     - Console commands
IP          - IP commands
>
>IP
IP>?
Commands at IP level:
IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]
IP Status
IP Ping [-n <count>] [-w <timeout>] <ipaddress>
IP Dhcp [enable|disable]
IP tftpget server-ip filename
```

System Restore Default

The **System Restore Default** command resets the device configuration to factory defaults. Adding the **keepIP** option retains the IP address of the switch.

Syntax

[System] restore default [*keep IP*]

Parameters

- *keep IP* – retain the same IP address after returning to factory settings.

Default Configuration

This command has no default configuration.

User Guidelines

The system does not prompt for confirmation of the request. The switch is not rebooted.

Example

The following displays the list presented for the **system restore default** command:

```
System>restore default
*** Restoring to default configuration...
*** Restored to default configuration...
*** Activating new configuration...
System>
```

System Reboot

The **System Reboot** command simulates a power cycle of the device

Syntax

[System] reboot

Default Configuration

This command has no default configuration.

User Guidelines

The system does not prompt for confirmation of the request.

Example

The following displays the list presented for the **system reboot** command:

```
System>reboot
System>
Booting ...image 1
SRAM testing: Passed
S/W Version: occ01_00_00
H/W Version: R01
serial number0001
Default IP address: 169.254.17.16
**Bootup finish**

Username:
```

Console Password

The **Console Password** command changes the user's password

Syntax

[Console] Password [*password*]

Parameters

- *password* – the new password to be assigned.

Default Configuration

This command has no default configuration.

User Guidelines

Entering the password command without supplying a new password will display the current password. To remove the password it is necessary to restore the unit back to factory defaults. See the **System Restore** Command.

Example

The following displays the list presented for the **Console password** command:

```
>console
Console>password admin
Console>password
Password: admin
Console>
```

IP Setup

The **IP Setup** command allows the user to display the IP address settings or to define a manual IP address on the device.

Syntax

[IP] setup [<ipaddress>][<ipmask>][<ipgateway>] [<vid>]

Parameters

- *ipaddress* – IP address to assign
- *ipmask* – IP subnet mask to assign
- *ipgateway* – IP gateway to assign
- *vid* – VLAN ID. This value should only be set to 1 if specified

Default Configuration

The device will by default attempt to get an IP address from a dhcp server. If this fails it will use a default IP address of 169.254.xx.yy, where xx and yy are the last two bytes of the MAC address (see label on the underside of your switch).

User Guidelines

Entering the IP setup command without any associated parameters will result in the switch displaying the current IP settings. If the unit has obtained an IP address from a dhcp server, entering a manual IP address will not change the IP address of the unit until the dhcp mode is disabled, as dhcp will override the manual IP address assignment. Refer to the **IP dhcp** command.

Example

The following displays the list presented for the **IP Setup** command, reviewing and assigning a manual IP address:

```
IP>setup
    Address: 169.254.17.16
    Subnet Mask: 255.255.0.0
    Gateway: 0.0.0.0
    VID: 1
IP>dhcp disable
IP>setup 192.168.1.2 255.255.255.0 192.168.1.1
IP>setup
    Address: 192.168.1.2
    Subnet Mask: 255.255.255.0
    Gateway: 192.168.1.1
    VID: 1
IP>
```

IP Status

The **IP Status** command allows the user to display the IP address settings on the device.

Syntax

[IP] status

Default Configuration

This command has no default configuration.

User Guidelines

Entering the IP setup command without supplying a manual IP address will result in the switch displaying the current IP settings. If the unit has obtained an IP address from a dhcp server, entering a manual IP address will not change the IP address of the unit until the dhcp mode is disabled, as dhcp will override the manual IP address assignment. Refer to the **IP dhcp** command.

Example

The following displays the list presented for the **IP Status** command:

```
IP>status
    IP Method:   Manual (DHCP disabled)
    IP Address:  192.168.1.2
    Subnet Mask: 255.255.0.0
    Gateway:     192.168.1.1
    Mgmt VID:    1
IP>
```

IP Ping

The **IP Ping** command sends ICMP echo request packets to another node in the network.

Syntax

[IP] Ping *[-n <count>] [-w <timeout>] <ipaddress>*

Parameters

- *count* – the number of echo requests to send
- *timeout* – timeout in seconds to wait for each reply
- *ipaddress* – IP address to ping

Default Configuration

This command has no default configuration.

User Guidelines

The maximum timeout is 60 seconds.

Example

The following displays the list presented for the **IP Ping** command:

```
IP>ping -n 2 -w 10 192.168.1.1
Reply from 192.168.1.1, packet     1, time     7 ms
Reply from 192.168.1.1, packet     2, time     8 ms
IP>
```

IP Dhcp

The **IP dhcp** command enables or disables the switch from obtaining an IP address from a dhcp server on the network

Syntax

[IP] dhcp *[enable] [disable]*

Parameters

- *enable* – enables the dhcp function
- *disable* – disables the switch from using a dhcp server to obtain an IP address. The switch will revert to the manually assigned IP address

Default Configuration

Entering this command without any parameters will display the current status of the dhcp mode.

User Guidelines

Setting dhcp to **enable** will override any manual IP address settings that may have been assigned.

Example

The following displays the list presented for the **IP dhcp** command:

```
IP>dhcp enable
Reply from 192.168.1.1, packet     1, time     7 ms
Reply from 192.168.1.1, packet     2, time     8 ms
IP>
```

IP tftpget

The **IP tftpget** command starts a firmware download for system upgrading or replacing corrupted firmware.

Syntax

[IP] tftpget *<tftp server ip address> <filename>*

Parameters

- *tftp server ip address* – the address of the workstation hosting the tftp server
- *filename* – the name of the software to be downloaded.

Default Configuration

This command has no default configuration.

User Guidelines

The TFTP server IP address and the software image file name on the server must be specified. During the upgrade process, a series of '.' symbols appear representing the upgrade process in the CLI interface. When the upgrade process is completed, the switch will re-boot. Press **Return** for the login prompt.

Example

The following displays the list presented for the **ftptget** command:

```
IP>tftpget 192.168.1.1 oc801_00_00.bin
TFTP transfer starting
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
..............File transfer completed
IP>Firmware upload in success, rebooting ...

Booting ...image 1
SRAM testing: Passed

S/W Version: V1.0.0
H/W Version: R01
serial number0001
Default IP address: 169.254.17.16
**Bootup finish**....
```

IP tftpput

The **IP tftpput** command copies either the backup configuration file or the current runtime software to a tftp server.

Syntax

[IP] tftpput [config¦ image] <*tftp server ip address*> <*filename*>

Parameters

- *config* – Selects the backup configuration option
- *image* – Selects the software image backup option
- *tftp server ip address* – the address of the workstation hosting the tftp server
- *filename* – the name of the file being saved.

Default Configuration

This command has no default configuration.

User Guidelines

The option of **config** or **image,** TFTP server IP address and the destination file name on the server must be specified. During the firmare backup process, a series of '.' symbols

appear representing the backup process in the CLI interface. Note that the configuration backup file is not a text file and cannot be edited.

Example

The following displays the list presented for the **ftppput** command:

```
IP>tftpput config 192.168.1. backup_config
TFTP transfer starting
...File transfer completed
IP>
IP>tftpput image 192.168.1.1 runtime.bin
TFTP transfer starting
.............................................................
.............................................................
.............................. .....File transfer completed
IP>
```

17 TROUBLESHOOTING

This section describes problems that may arise when installing the and how to resolve these issue. This section includes the following topics:

- **Problem Management** — Provides information about problem management.
- **Troubleshooting Solutions** — Provides a list of troubleshooting issues and solutions for using the device.

Problem Management

Problem management includes isolating problems, quantifying the problems, and then applying the solution. When a problem is detected, the exact nature of the problem must be determined. This includes how the problem is detected, and what are the possible causes of the problem. With the problem known, the effect of the problem is recorded with all known results from the problem. Once the problem is quantified, the solution is applied. Solutions are found either in this chapter, or through customer support. If no solution is found in this chapter, contact Customer Support.

Troubleshooting Solutions

Listed below are some possible troubleshooting problems and solutions. These error messages include:

- Cannot connect to management using RS-232 serial connection
- Cannot connect to switch management using HTTP, SNMP, etc.
- Self-test exceeds 15 seconds
- No connection is established and the port LED is on
- Device is in a reboot loop
- No connection and the port LED is off
- Lost Password.

Problems	Possible Cause	Solution
Cannot connect to management using RS-232 serial connection		Be sure the terminal emulator program is set to VT-100 compatible, 38400 baud rate, no parity, 8 data bits and one stop bit Use the included cable, or be sure that the pin-out complies with a standard null-modem cable
Cannot connect to switch management using HTTP, SNMP, etc.		Be sure the switch has a valid IP address, subnet mask and default gateway configured Check that your cable is properly connected with a valid link light, and that the port has not been disabled Ensure that your management station is plugged into the appropriate VLAN to manage the device If you cannot connect using the web, the maximum number of connections may already be open. Please try again at a later time.
No response from the terminal emulation software	Faulty serial cable Incorrect serial cable Software settings	Replace the serial cable Replace serial cable for a pin-to-pin straight/flat cable Reconfigure the emulation software connection settings.
Response from the terminal emulations software is not readable	Faulty serial cable Software settings	Replace the serial cable Reconfigure the emulation software connection settings.
Self-test exceeds 15 seconds	The device may not be correctly installed.	Remove and reinstall the device. If that does not help, consult your technical support representative.
No connection is established and the port LED is on	Wrong network address in the workstation No network address set Wrong or missing protocol Faulty Ethernet cable Faulty port Faulty module Incorrect initial configuration	Configure the network address in the workstation Configure the network address in the workstation Configure the workstation with IP protocol Replace the cable Replace the module Replace the module Erase the connection and reconfigure the port
Device is in a reboot loop	Software fault	Download and install a working or previous software version from the console

<table>
<tr><th>Problems</th><th>Possible Cause</th><th>Solution</th></tr>
<tr><td>No connection and the port LED is off</td><td>Incorrect Ethernet cable, e.g., crossed rather than straight cable, or vice versa, split pair (incorrect twisting of pairs)
Fiber optical cable connection is reversed
Bad cable
Wrong cable type</td><td>Check pinout and replace if necessary
Change if necessary. Check Rx and Tx on fiber optic cable
Replace with a tested cable
Verify that all 10 Mbps connections use a Cat 5 cable
Check the port LED or zoom screen in the NMS application, and change setting if necessary</td></tr>
<tr><td>Lost Username and/or Password</td><td colspan="2">Note: By following this procedure you will also erase all the configuration settings you may have. The username and password are stored in the configuration file (you cannot see them as the file is not readable). If you restore your configuration file after having followed the procedure below, you will reset the username/password back to what it was before.
If you have forgotten the username and/or the password, you can reset these back to the default values (Username=admin, no password) by entering the safe mode when the switch is booting up.
When the switch is booting up, immediately after the first message (<code>Booting ...image 0</code>) is displayed, press together the Control, Shift and – keys. If you have been successful, you will see the output below on the console interface. If you do not get the <code>Entering safe mode</code> displayed, power cycle the switch and try again.
<pre>Booting ...image 0
Entering safe mode
SRAM testing: Passed
S/W Version: V1.0.0
H/W Version: R01
serial number0001
Default IP address: 169.254.0.1
Bootup finish
Entered safe mode</pre>Note The software and hardware versions, serial number and default IP address on your switch are likely to be different to those shown in the above example.
You now have access to a limited set of commands that do not require you to login in to gain access to them.
Enter the command: <code>system restore default</code>
This will delete all the configuration files and return the switch to it’s factory default state.
The console will display:
<pre>>system restore default
*** Restoring to default configuration...
*** Restored to default configuration...
*** Activating new configuration...</pre>Enter the command: <code>exit</code>
This will exit the safe mode and you can now log back into the switch with the username “admin” and no password.</td></tr>
</table>

18 OBTAINING SUPPORT FOR YOUR 3COM PRODUCT

3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

Register Your Product to Gain Service Benefits

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

Warranty and other service benefits are enabled through product registration. Register your product at **http://eSupport.3com.com/**. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request. If you have trouble registering your product, please contact 3Com Global Services for assistance.

Troubleshoot Online

You will find support tools posted on the 3Com Web site at **www.3Com.com**

3Com Knowledgebase — Helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

http://knowledgebase.3com.com

It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services like 3Com Express[SM] and Guardian[SM] can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects.

More information on 3Com maintenance and Professional Services is available at **www.3com.com**.

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

Software Updates are the bug fix/maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com Web site at **http://eSupport.3com.com/**.

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://eSupport.3com.com/**, or under the Product Support heading at **www.3com.com/**

Software Upgrades are the feature releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

http://eSupport.3com.com/

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at http://eSupport.3com.com/. First-time users must apply for a user name and password.

Contact Us

3Com offers telephone, internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

http://csoweb4.3com.com/contactus/

Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair	
Australia	1800 075 316
Hong Kong	2907 0456
India	000 800 440 1193
Indonesia	001 803 852 9825
Japan	03 3507 5984
Malaysia	1800 812 612
New Zealand	0800 450 454
Philippines	1800 144 10220 or 029003078
PR of China	800 810 0504
Singapore	800 448 1433
South. Korea	080 698 0880
Taiwan	00801 444 318
Thailand	001 800 441 2152
Pakistan Call the U.S. direct by dialing 00 800 01001, then dialing 800 763 6780	
Sri Lanka Call the U.S. direct by dialing 02 430 430, then dialing 800 763 6780	
Vietnam Call the U.S. direct by dialing 1 201 0288, then dialing 800 763 6780	
You can also obtain non-urgent support in this region at this email address **apr_technical_support@3com.com** Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048, or send an email at this email address: **ap_rma_request@3com.com**	

Country	Telephone Number
Europe, Middle East, and Africa – Telephone Technical Support and Repair	
From anywhere in these regions not listed below, call: +44 1442 435529	
From the following countries, call the appropriate number:	
Austria	0800 297 468
Belgium	0800 71429
Denmark	800 17309
Finland	0800 113153
France	0800 917959
Germany	0800 182 1502
Hungary	06800 12813
Ireland	1 800 533 117
Israel	180 945 3794
Italy	0800 879489
Luxembourg	800 23625
Netherlands	0800 0227788
Norway	800 11376
Poland	00800 4411 357
Portugal	800 831416
Russia	88005558588
Saudi Arabia	800 8 445 312
South Africa	0800 995 014
Spain	900 938 919
Sweden	020 795 482
Switzerland	0800 553 072
U.A.E.	04-3908997

Country	Telephone Number
U.K.	0800 096 3266
You can also obtain support in this region using this URL: **http://emea.3com.com/support/email.html** You can also obtain non-urgent support in this region at these email addresses: Technical support and general requests: **customer_support@3com.com** Return material authorization number: **warranty_repair@3com.com** Contact Requests: **emea_contact@3com.com**	

Country	Telephone Number
Latin America – Telephone Technical Support and Repair	
Antigua	AT&T +800 988 2112
Antigua Barbuda	AT&T +800 988 2112
Argentina	AT&T +800 988 2112
Aruba	AT&T +800 988 2112
Bahamas	AT&T +800 988 2112
Barbados	AT&T +800 988 2112
Belize	AT&T +800 988 2112
Bermuda	AT&T +800 988 2112
Bolivia	AT&T +800 988 2112
Brasil	0800-133266 (0800-13-3COM)
Brasil Local	+5511 5643 2700
British Virgin Islands	AT&T +800 988 2112
Cayman Islands	AT&T +800 988 2112
Chile	AT&T +800 988 2112
Colombia	AT&T +800 988 2112
Colombia Local	+571 592 5000
Costa Rica	AT&T +800 988 2112
Curaço	AT&T +800 988 2112
Dominican Republic	AT&T +800 988 2112
El Salvador	AT&T +800 988 2112
Equator	AT&T +800 988 2112
French Guyana	AT&T +800 988 2112
Grenada	AT&T +800 988 2112
Guadalupe	AT&T +800 988 2112
Guatemala	AT&T +800 988 2112
Guyana	AT&T +800 988 2112
Haiti	AT&T +800 988 2112
Honduras	AT&T +800 988 2112
Jamaica	AT&T +800 988 2112
Mexico	1800 849 2273
Mexico Local	+52-55-52-01-0004
Monserrat	AT&T +800 988 2112
Nicaragua	AT&T +800 988 2112
Panama	AT&T +800 988 2112
Paraguay	AT&T +800 988 2112
Peru	AT&T +800 988 2112
Puerto Rico	AT&T +800 988 2112
Rest of Latin America	+1 508 323 6234
St. Kitts Nevis	AT&T +800 988 2112
St. Lucia	AT&T +800 988 2112
St. Vincent	AT&T +800 988 2112
Suriname	AT&T +800 988 2112
Trinidad and Tobago	AT&T +800 988 2112
Turks and Caicos	AT&T +800 988 2112
Uruguay – Montivideo	AT&T +800 988 2112
Venezuela	AT&T +800 988 2112

Country	Telephone Number
Virgin Islands	AT&T +800 988 2112

You can also obtain support in this region in the following ways:

Spanish speakers, enter the URL:
http://lat.3com.com/lat/support/form.html

Portuguese speakers, enter the URL:
http://lat.3com.com/br/support/form.html

English speakers in Latin America should send an e-mail to:
lat_support_anc@3com.com

Country	Telephone Number
US and Canada – Telephone Technical Support and Repair	
All locations:	
Network Jacks; Wired	1 847 262 0070
All other 3Com products	1 800 876 3226

19 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.

ICES STATEMENT

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

Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

CE STATEMENT (EUROPE)

3Com Europe Limited
Peoplebuilding 2,
Peoplebuilding Estate
Maylands Avenue
Hemel Hempstead,
Hertfordshire
HP2 4NW
United Kingdom

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.

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

A copy of the signed Declaration of Conformity can be downloaded from the Product Support web page for the OfficeConnect Managed Gigabit Switch (3CDSG8) at http://www.3Com.com.

Also available at http://support.3com.com/doc/3CDSG8_EU_DOC.pdf