3Com® OfficeConnect Managed PoE Switch

User Guide

3CRDSF9PWR

www.3Com.com
Part Number 10016863 Rev. BA
Published August 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.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE 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 Fast Ethernet PoE 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 Fast Ethernet PoE Switch and how it can be used in your network. It covers summaries of hardware and software features.
- **Using the 3Com Web Interface** — Provides information for using the Web interface including adding, editing, and deleting device configuration information.
- **Viewing Basic Settings** — provides information for viewing and configuring essential information required for setting up and maintaining device settings.
- **Managing Device Security** — Provides information for configuring both system and network security, including traffic control, ACLs, and device access methods.
- **Managing System Information** — Provides information for configuring general system information including the user-defined system name, the user-defined system location, and the system contact person.
- **Configuring Ports** — Provides information for configuring port settings.

- **Aggregating Ports** — Provides information for configuring Link Aggregation which optimizes port usage by linking a group of ports together to form a single LAG.
- **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.
- **Configuring IP and MAC Address Information** — Provides information for configuring IP addresses, DHCP and ARP.
- **Configuring IGMP Snooping** — Provides information for configuring IGMP Snooping and IGMP Query.
- **Configuring Spanning Tree** — Provides information for configuring Classic and Rapid Spanning Tree.
- **Configuring SNMP** — Provides information for configuring the *Simple Network Management Protocol* (SNMP) which provides a method for managing network devices.
- **Configuring Quality of Service** — Provides information defining Quality of Service, including default CoS values, queue service mode, DSCP and CoS mapping, Trust mode, bandwidth settings, and Voice VLAN.
- **Managing System Files** — Provides information for defining file maintenance.
- **Managing Power over Ethernet Devices** — Provides information for specifying which ports are authorized PoE service, and the service priority.
- **Managing System Logs** — Provides information for viewing system logs, and configuring device log servers.
- **Viewing Statistics** — Provides information for viewing interface and RMON statistics.
- **Managing Device Diagnostics** — Provides information for managing device diagnostics, including port mirroring, cable testing, and pinging remote 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
ℹ	Information note	Information that describes important features or instructions.
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
⚡	Warning	Information that alerts you to potential personal injury.

Related Documentation

In addition to this guide, other documentation available for the 3Com® OfficeConnect Managed Fast Ethernet PoE Switch include the following:

- *Safety and Regulatory Information*: Provides installation, set-up, and regulatory compliance information.

CONTENTS

ABOUT THIS GUIDE

1 GETTING STARTED

2 Using the 3Com Web Interface

3 Viewing Basic Settings

4 Managing Device Security

5 Managing System Information

6 Configuring Ports

12 CONFIGURING SNMP

13 CONFIGURING QUALITY OF SERVICE

14 MANAGING SYSTEM FILES

15 MANAGING POWER OVER ETHERNET DEVICES

16 MANAGING SYSTEM LOGS

17 VIEWING STATISTICS

18 MANAGING DEVICE DIAGNOSTICS

A 3COM NETWORK MANAGEMENT

B DEVICE SPECIFICATIONS AND FEATURES

C PIN-OUTS

D Troubleshooting

E Glossary

F Obtaining Support for Your 3Com Products

Regulatory Notices

1 GETTING STARTED

This chapter contains introductory information about the 3Com® OfficeConnect Managed Fast Ethernet PoE Switch and how it can be used in your network. It covers summaries of hardware and software features and also the following topics:

- About the OfficeConnect Managed Fast Ethernet PoE 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 Command Line Interface Management
- Setting Up SNMP Management V1 or V2
- Default Users and Passwords
- Upgrading Software using the CLI

About the OfficeConnect Managed Fast Ethernet PoE Switch

The OfficeConnect Managed Fast Ethernet PoE Switch is a switching product that delivers flexible three-speed performance (10/100/1000), Power over Ethernet (PoE and PoE Plus) and advanced voice-optimized features such as auto-QoS and auto-voice VLAN. This makes the switch ideal for small enterprises seeking to build a secure converged network.

The OfficeConnect Managed Fast Ethernet PoE Switch includes the following model:

- OfficeConnect Managed Fast Ethernet PoE Switch (9-Port)

The OfficeConnect Managed Fast Ethernet PoE Switch features the following advantages:

- Eight Fast Ethernet access ports
- One Gigabit Ethernet uplink port
- Port security
- Link aggregation control protocol (LACP)
- Up to 256 VLANs
- Access control lists (ACLs)
- Port access control through IEEE 802.1X or local database
- Port-based mirroring

Summary of Hardware Features

Table 1 summarizes the hardware features supported by the OfficeConnect Managed Fast Ethernet PoE Switch.

Table 1 Hardware Features

Feature	OfficeConnect Managed Fast Ethernet 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 RJ-45 ports
Auto MDI/MDIX	Supported on all RJ-45 ports. If fiber SFP transceivers are used, Auto MDIX is not supported.
Flow Control	In full duplex operation all ports are supported. The Gigabit switch ports are capable of receiving, but not sending pause frames.

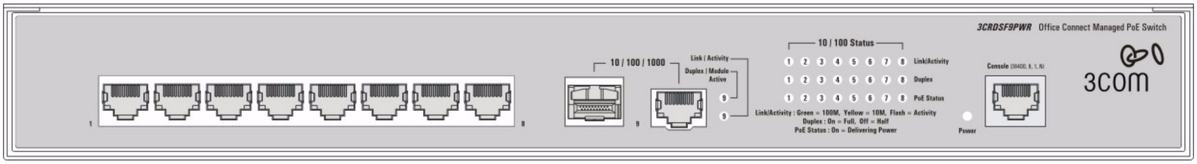
Table 1 Hardware Features (continued)

Feature	OfficeConnect Managed Fast Ethernet PoE Switch
Traffic Prioritization	Supported (using the IEEE Std 802.ID, 1998 Edition): Four traffic queues per port
Power over Ethernet and Power over Ethernet Plus	Supported on ports 1-8
Fast Ethernet Ports	Auto-negotiating 10/100BASE-TX ports
Gigabit Ethernet Ports	Auto-negotiating 10/100/1000BASE-T ports
SFP Ethernet Port	Supports fiber Gigabit Ethernet long-wave (LX), fiber Gigabit Ethernet short-wave (SX), and single-strand fiber Fast Ethernet (BX) transceivers.
Mounting	Standalone and rack mounting

Front Panel Detail

Figure 1 shows the front panel of the OfficeConnect Managed Fast Ethernet PoE Switch 9-Port unit.

Figure 1 OfficeConnect Managed Fast Ethernet PoE Switch—front panel.


3CRDSF9PWR Office Connect Managed PoE Switch
1
8
10 / 100 / 1000
9
Link / Activity
Duplex / Module Active
9
9
10 / 100 Status
1 2 3 4 5 6 7 8 Link/Activity
1 2 3 4 5 6 7 8 Duplex
1 2 3 4 5 6 7 8 PoE Status
Link/Activity : Green = 100M, Yellow = 10M, Flash = Activity
Duplex : On = Full, Off = Half
PoE Status : On = Delivering Power
Power
Console (38400, 8, 1, N)
3com

LED Status Indicators

The OfficeConnect Managed Fast Ethernet PoE 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 on the LEDs of the OfficeConnect Managed Fast Ethernet PoE Switch

LED	Label	Status	Description
Power	Power	Green	The switch starts normally. The LED flashes when the system is performing power-on self test (POST) or firmware is being upgraded.
		Yellow	The system has failed the POST.
		OFF	The switch is powered off.
10/100 BASE-TX Ethernet port status	Link/ Activity	Green	The port works at the rate of 100 Mbps; the LED flashes quickly when the port is sending or receiving data.
		Yellow	The port works at the rate of 10 Mbps; the LED flashes quickly when the port is sending or receiving data.
		OFF	The port is not connected.
10/100/1000 BASE-T Ethernet port status	Link/ Activity	Green	The port works at the rate of 1000 Mbps; the LED flashes quickly when the port is sending or receiving data.
		Yellow	The port works at the rate of 10/100 Mbps; the LED flashes quickly when the port is sending or receiving data.
		OFF	The port is not connected.
Duplex mode	Duplex	Yellow	The port is in full duplex mode.
		OFF	The port is not connected, or is in half duplex mode.
100/1000 Base SFP port status	Module Active	Green	An SFP module is inserted.
		OFF	An SFP module is not inserted or is not recognized.
PoE status	PoE Status	Green	Delivering power. The LED flashes if a fault occurs.
		OFF	Not delivering power.

System Specifications

Table 3 contains the system specifications of the OfficeConnect Managed Fast Ethernet PoE switch.

Table 3 System specifications of the OfficeConnect Managed Fast Ethernet PoE switch

Specification	OfficeConnect Managed Fast Ethernet PoE Switch
Physical dimensions (W×D×H)	440×265×43.6 mm (17.3x10.4x1.7 in.)
Weight	2.04 kg (4.50 lb)
Console port	One Console port
Fast Ethernet ports on the front panel	8 × 10/100 Mbps Ethernet ports
Gigabit Ethernet ports on the front panel	One 10/100/1000 Mbps Ethernet port (shared with the SFP port)
SFP ports on the front panel	One 100/1000 Mbps SFP port (shared with the Gigabit Ethernet RJ-45 port)
AC Input voltage	Rated voltage range: 100–240 VAC, 50/60 Hz
Power consumption (full load)	200.3 BTU/hr (88 Watts)
Operating temperature	0 to 40 °C (32 to 113 °F)
Relative humidity	0 to 95% noncondensing

Additional specifications can be found in Appendix B “Device Specifications and Features”.

Approved SFP Transceivers

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

- 3CSFP91 SFP (1000BASE-SX)
- 3CSFP92 SFP (1000BASE-LX)
- 3CSFP85 and 3CSFP86 SFP (100BASE-BX)

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

http://www.3com.com

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
- Using the Command Line Interface (CLI)
- Manually set the IP Address using the Console Port
- Viewing IP Information using the Console Port
- Setting Up Web Interface Management
- Setting Up Command Line Interface Management
- Setting Up SNMP Management V1 or V2
- Default Users and Passwords

Methods of Managing a Switch

To manage your switch you can use one of the following methods:

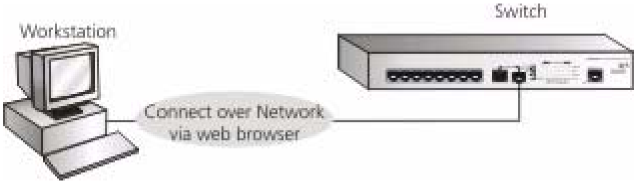
- Web Interface Management
- Command Line Interface Management
- SNMP Management

You can use the Command Line Interface through the Console port for complete access to all operations of the switch including setting and viewing the IP address, configuring user accounts, upgrading switch firmware, and more. Refer to the *3Com CLI Reference Guide*.

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 (see Figure 2).

Figure 2 Web Interface Management over the Network



Refer to "Setting Up Web Interface Management" on page 30.

Command Line Interface Management

Each switch has a command line interface (CLI) that allows you to manage the switch from a workstation, either locally via a console port connection (see Figure 3), or remotely over the network (see Figure 4).

Figure 3 CLI management via the console port

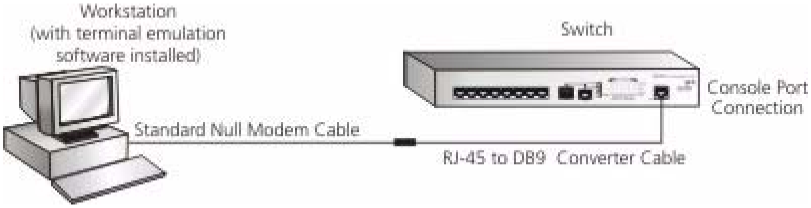
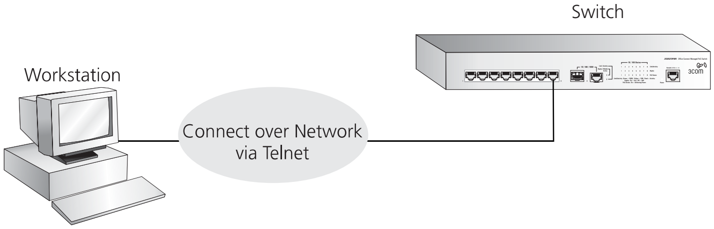


Figure 4 CLI management over the network

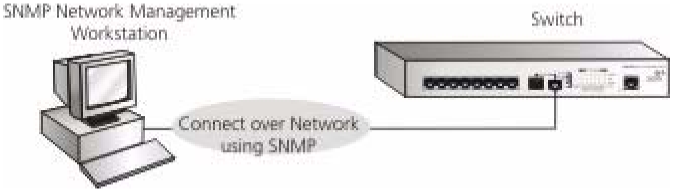


Refer to "Setting Up Command Line Interface Management" on page 31.

SNMP Management

You can manage a switch using any network management workstation running the Simple Network Management Protocol (SNMP) as shown in Figure 5. For example, you can use the 3Com Network Director software, available from the 3Com web site.

Figure 5 SNMP Management over the Network


SNMP Network Management Workstation
Switch
Connect over Network using SNMP

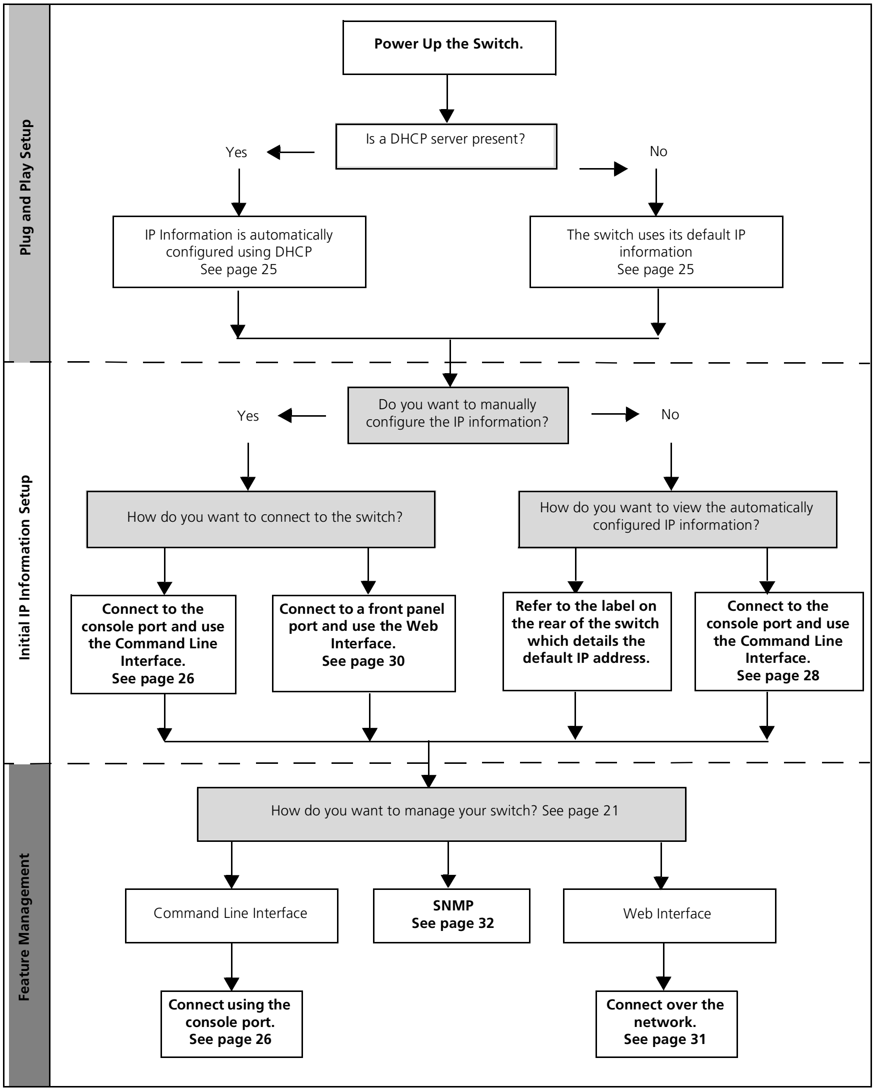
Refer to "Setting Up SNMP Management V1 or V2" on page 32.

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. The whole setup process is summarized in Figure 6. 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
- Prepare for your chosen method of management

Figure 6 Initial Switch Setup and Management Flow Diagram


Plug and Play Setup
Power Up the Switch.
Is a DHCP server present?
Yes
No
IP Information is automatically configured using DHCP See page 25
The switch uses its default IP information See page 25
Initial IP Information Setup
Do you want to manually configure the IP information?
Yes
No
How do you want to connect to the switch?
How do you want to view the automatically configured IP information?
Connect to the console port and use the Command Line Interface. See page 26
Connect to a front panel port and use the Web Interface. See page 30
Refer to the label on the rear of the switch which details the default IP address.
Connect to the console port and use the Command Line Interface. See page 28
Feature Management
How do you want to manage your switch? See page 21
Command Line Interface
SNMP See page 32
Web Interface
Connect using the console port. See page 26
Connect over the network. See page 31

***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 "Default Users and Passwords" on page 33.*

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 bottom and top 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 "Viewing IP Information using the Console Port" on page 28.

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 "Manually set the IP Address using the Console Port" on page 27.

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 the 3Com CLI Reference Guide.

Connecting to the Console Port

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

Prerequisites

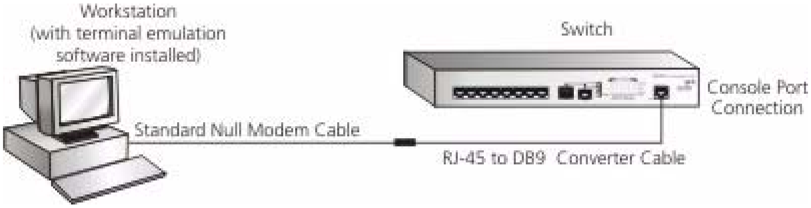
- A workstation with terminal emulation software installed, such as Microsoft Hyperterminal. This software allows you to communicate with the switch using the console port directly.
- Documentation supplied with the terminal emulation software.
- The console cable (RJ-45 to DB-9) supplied with your switch.

You can find pin-out diagrams for the cable in Appendix C on page 235.

Connecting the Workstation to the Switch

1 Connect the workstation to the console port using the console cable as shown in Figure 7.

Figure 7 Connecting a Workstation to the switch using the Console Port


Workstation (with terminal emulation software installed)
Switch
Console Port Connection
Standard Null Modem Cable
RJ-45 to DB9 Converter Cable

To connect the cable:

a Attach the cable's RJ-45 connector to the Console port of the switch.

b 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 Fast Ethernet PoE Switch takes approximately two minutes 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 26.

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 **Console#** prompt should be displayed.

5 Enter the following commands to enter configuration mode, specify the VLAN to which the IP address will be assigned, and then enter the IP address and subnet mask for the switch as follows:

```
Console#configure
Console(config)#interface vlan 1
Console(config-if)#ip address xxx.xxx.xxx.xxx
   mmm.mmm.mmm.mmm
```

(Note: xxx.xxx.xxx.xxx is the IP address and mmm.mmm.mmm.mmm is the subnet mask of the switch.)

6 Enter the **end** command to return to the Privileged Exec mode, and then enter the **quit** command to terminate the CLI session.

The initial setup 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 21.

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 26.

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, the **Console#** prompt is displayed.

5 Enter **show ip interface** to view a summary of the allocated IP address. The following is an example of the displayed information.

```
Console#show ip interface
 IP Address and Netmask: 169.254.99.51 255.255.0.0 on VLAN 1,
 Address Mode:            DHCP
Console#
```

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 21.

For more information about the CLI, refer to the 3Com CLI Reference Guide.

If you do not intend to use the command line interface using the console port to manage the switch, you can log out, 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 21.
- Ensure that the switch is connected to the network using a Category 5 twisted pair Ethernet cable with RJ-45 connectors.
- A suitable Web browser.

Choosing a Browser

To display the web interface correctly, use one of the following Web browser and platform combinations:

Table 4 Supported Web Browsers and Platforms

		Platform	
Browser	**Windows 2000**	**Windows XP**	**Windows Vista**
Internet Explorer 5.5 and above	Yes	Yes	Yes
Firefox 6 and above	Yes	Yes	Yes
Netscape 6.2 and above	Yes	Yes	Yes

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.

The switch's Web interface supports both secure (HTTPS) and non-secure (HTTP) connections.

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 25, and "Viewing IP Information using the Console Port" on page 28.
2. Check that your management workstation is on the same subnet as your switch.
3. Check that 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 password).

   The main Web interface page is displayed.

Setting Up Command Line Interface Management

This section describes how you can set up command line interface management using a local console port connection or over the network.

CLI Management via the Console Port

To manage a switch using the command line interface via the local console port connection:

1. Ensure you have connected your workstation to the console port correctly as described in "Connecting to the Console Port" on page 26.
2. Your switch is now ready to continue being managed and/or configured through the CLI via its console port.

CLI Management over the Network

To manage a switch using the command line interface over a network using Telnet:

1. Ensure you have already set up the switch with IP information as described in "Methods of Managing a Switch" on page 21.
2. Check that you have the IP protocol correctly installed on your management workstation. You can check this by trying to browse the World Wide Web. If you can browse, the IP protocol is installed.
3. Check that you can communicate with the switch by entering a **`ping`** command at the DOS prompt in the following format:

   ```
   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. To open a Telnet session via the DOS prompt, enter the IP address of the switch that you wish to manage in the following format:

   ```
   telnet xxx.xxx.xxx.xxx
   ```

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

   If opening a Telnet session via third party software you will need to enter the IP address in the format suitable for that software.
5. At the login and password prompts, enter **`admin`** as your user name and enter your password at the password prompt (or just press Return if you have not yet set a password).

   If the login prompt does not display immediately, press Return a few times until it starts.
6. If you have logged on correctly, the **Console#** prompt will be displayed.

Setting Up SNMP Management V1 or V2

You can use any network management application running the Simple Network Management Protocol (SNMP) to manage the switch. 3Com offers a range of network management applications to address networks of all sizes and complexity. See "3Com Network Management" on page 225.

Be sure the management workstation is connected to the switch using a port in VLAN 1 (the Default VLAN). By default, all ports on the switch are in VLAN 1.

To display and configure SNMP management parameters, refer to *"Configuring SNMP"* on page 163.

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 two default user names. The default users are listed in Table 5.

Table 5 Default Users

User Name	Default Password	Access Level
admin	(no password)	Management — The user can access and change all manageable parameters
monitor	monitor	Monitor — the user can view all manageable parameters, but cannot change any manageable parameters

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

Changing Default Passwords

You can change the default passwords using either:

- The **`username`** command on the CLI, or
- The *Administration* > *System Access* > *Modify* operation on the web interface.

Upgrading Software using the CLI

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

Note: You can also upgrade the software using the switch Web user interface. See "Restoring the Software Image" page 197. Bootcode can only be upgraded using the CLI, for which instructions are supplied in the release notes.

1 To download the runtime application file, enter the following commands:

```
Console#copy tftp file
TFTP server IP address: aaa.aaa.aaa.aaa
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: rrr
Destination file name: rrr
```

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

2. When downloading a new runtime file, it will automatically overwrite the previous version. To set the switch to boot from the new runtime file you have downloaded, enter the **reload** command as shown below:

```
Console(config)#end
Console#reload
```

The following prompt displays:

```
System will be restarted, continue <y/n>?
```

3. Enter **y** and press Return. The system reboots the switch.

2 USING THE 3COM WEB INTERFACE

This section provides an introduction to the user interface, and includes the following topics:

- Starting the 3Com Web Interface
- Understanding the 3Com Web Interface
- Using Screen and Table Options
- Saving the Configuration
- Resetting the Device
- Restoring Factory Defaults
- Logging Off the Device

Starting the 3Com Web Interface

This section includes the following topics:

- Multi-Session Web Connections
- Accessing the 3Com Web Interface

Multi-Session Web Connections

The Multi-Session web connections feature enables 10 users to be created and access the switch concurrently. Access levels provide read or read/write permissions to users for configuring the switch. Users and access levels are described in *Configuring System Access*. Login information is always handled in the local database. A unique password is required of each user. Two access levels exist on the 3Com Web Interface:

- **Management access level** — Provides the user with read/write access. There is always one management level user configured for the switch. The factory default is be username: admin with no Password.
- **Monitor access level** — Provides the user with read-only access.

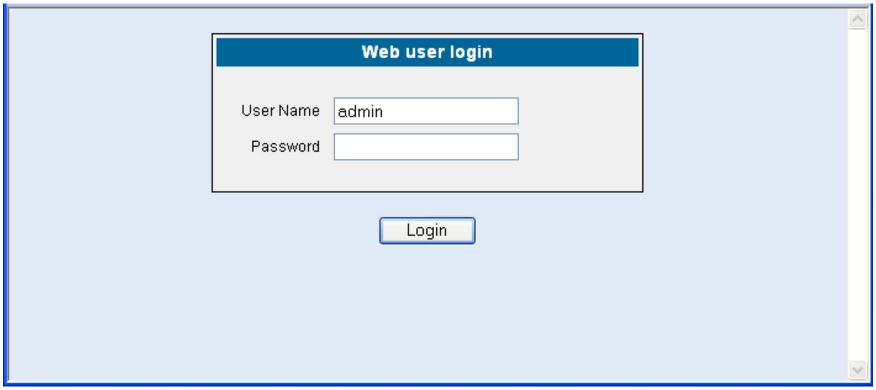
Accessing the 3Com Web Interface

This section contains information on starting the 3Com Web interface.

To access the 3Com user interface:

1. Open an Internet browser.
2. Enter the device IP address in the address bar and press Enter. The *Enter Network Password Page* opens:

Figure 8 Enter Network Password Page



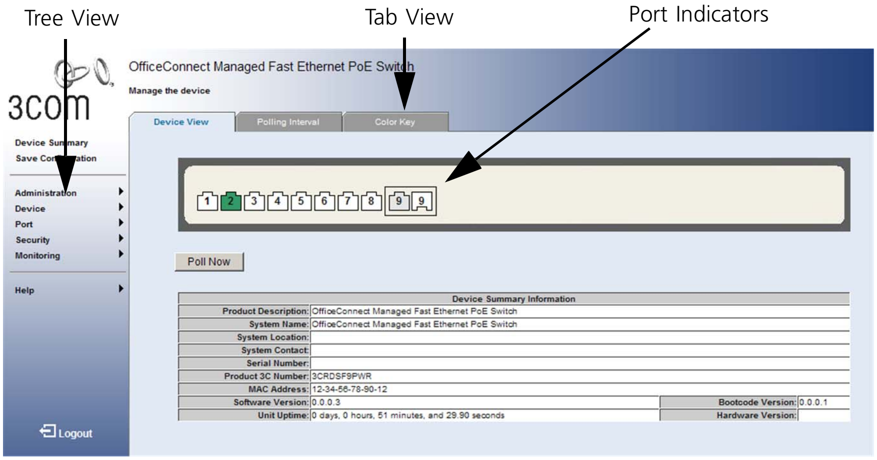
Web user login

User Name: admin

Password:

3. Enter your user name and password. The device default factory settings is configured with a User Name that is admin and a password that is blank. Passwords are case sensitive.

4 Click Login. The *3Com Web Interface Home Page* opens:



Device Summary Information			
Product Description:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Name:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Location:			
System Contact:			
Serial Number:			
Product 3C Number:	3CRDSF9PWR		
MAC Address:	12-34-56-78-90-12		
Software Version:	0.0.0.3	Bootcode Version:	0.0.0.1
Unit Uptime:	0 days, 0 hours, 51 minutes, and 29.90 seconds	Hardware Version:	

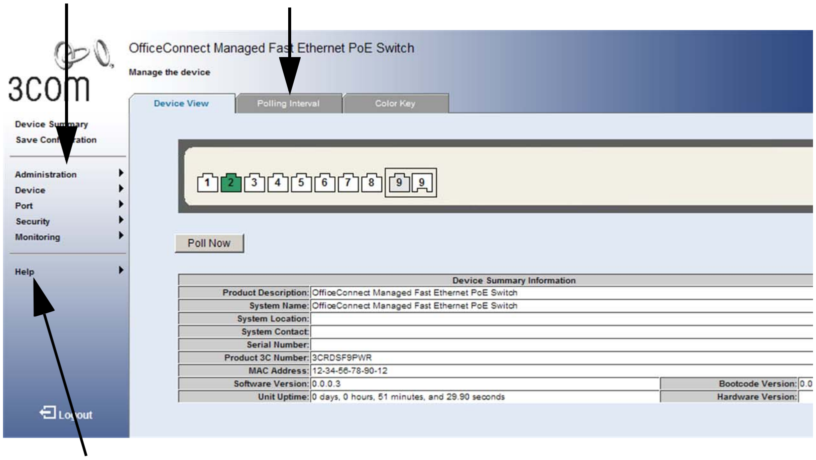
Figure 9 3Com Web Interface Home Page

Understanding the 3Com Web Interface

The *3Com Web Interface Home Page* contains the following views:

- **Tree View** — Provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
- **Tab View** — Provides the device summary information located at the top of the home page.
- **Port Indicators** — Located under the Device View at the top of the home page, the port indicators provide a visual representation of the ports on the front panel.

Figure 10 Web Interface Components



Device Summary Information			
Product Description:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Name:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Location:			
System Contact:			
Serial Number:			
Product 3C Number:	3CRDSF9PWR		
MAC Address:	12-34-56-78-90-12		
Software Version:	0.0.0.3	Bootcode Version:	0.0
Unit Uptime:	0 days, 0 hours, 51 minutes, and 29.90 seconds	Hardware Version:	

The following table lists the user interface components:

Table 6: Interface Components

View	Description
Tree View	Tree View provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
Tab View	The Tab Area enables navigation through the different device features. Click the tabs to view all the components under a specific feature.
Web Interface Information	Provides access to online help, and contains information about the Web Interface.

This section provides the following additional information:

- **Device Representation** — Provides an explanation of the user interface buttons, including both management buttons and task icons.
- **Using the 3Com Web Interface Management Buttons** — Provides instructions for adding, modifying, and deleting configuration parameters.

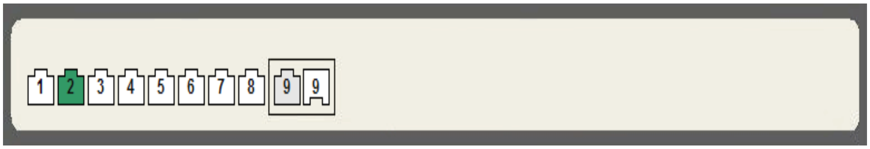
Device Representation

The *3Com Web Interface Home Page* contains a graphical panel representation of the device that appears within the Device View Tab.

To access the Device Representation:

1 Click **Device Summary > Device View**.

Figure 11 Device Representation



2 By moving your mouse over a port, you can view information about the port type, speed, duplex mode, utilization, and current status.

3 By selecting a specific port with your mouse, you can open the Port Administration Detail, Setup or Statistics (Summary) menu.

For detailed information on configuring ports, please refer to *Configuring Ports*.

Using the 3Com Web Interface Management Buttons

Configuration Management buttons and icons provide an easy method of configuring device information, and include the following:

Table 7: 3Com Web Interface Configuration Buttons

Button	Button Name	Description
Clear Logs	Clear Logs	Clears system logs.
Apply	Apply	Applies configuration changes to the device.
Remove	Remove	Deletes configuration settings.

Table 8: 3Com Web Interface Information Tabs

Tab	Tab Name	Description
Logout	Logout	Logs the user out and terminates the current session.

Using Screen and Table Options

3Com contains screens and tables for configuring devices. This section contains the following topics:

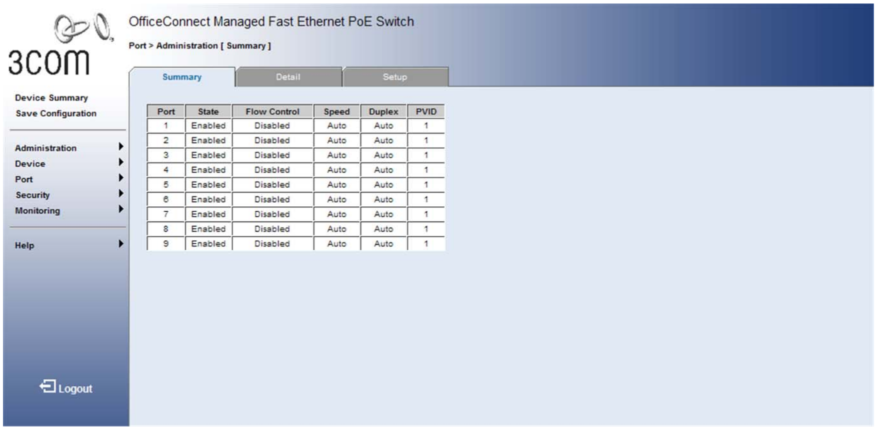
- Viewing Configuration Information
- Adding Configuration Information
- Modifying Configuration Information
- Removing Configuration Information

Viewing Configuration Information

To view configuration information:

1 Click **Port > Administration > Summary**. *The Port Settings Summary Page* opens:

Figure 12 Port Settings Summary Page



Port	State	Flow Control	Speed	Duplex	PVID
1	Enabled	Disabled	Auto	Auto	1
2	Enabled	Disabled	Auto	Auto	1
3	Enabled	Disabled	Auto	Auto	1
4	Enabled	Disabled	Auto	Auto	1
5	Enabled	Disabled	Auto	Auto	1
6	Enabled	Disabled	Auto	Auto	1
7	Enabled	Disabled	Auto	Auto	1
8	Enabled	Disabled	Auto	Auto	1
9	Enabled	Disabled	Auto	Auto	1

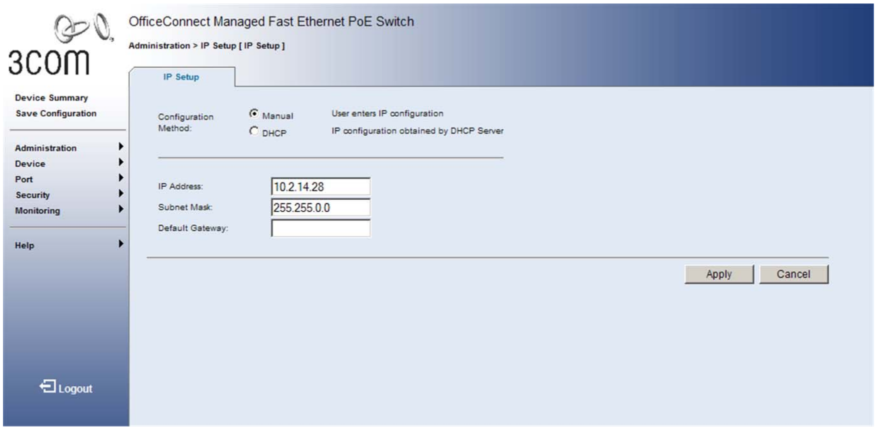
Adding Configuration Information

User-defined information can be added to specific 3Com Web Interface pages, by opening the *IP Setup Page*.

To configure IP Setup:

1 Click **Administration > IP Setup**. The *IP Setup Page* opens:

Figure 13 IP Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Administration > IP Setup [IP Setup]

Configuration Method: ● Manual User enters IP configuration
○ DHCP IP configuration obtained by DHCP Server

IP Address: 10.2.14.28
Subnet Mask: 255.255.0.0
Default Gateway:

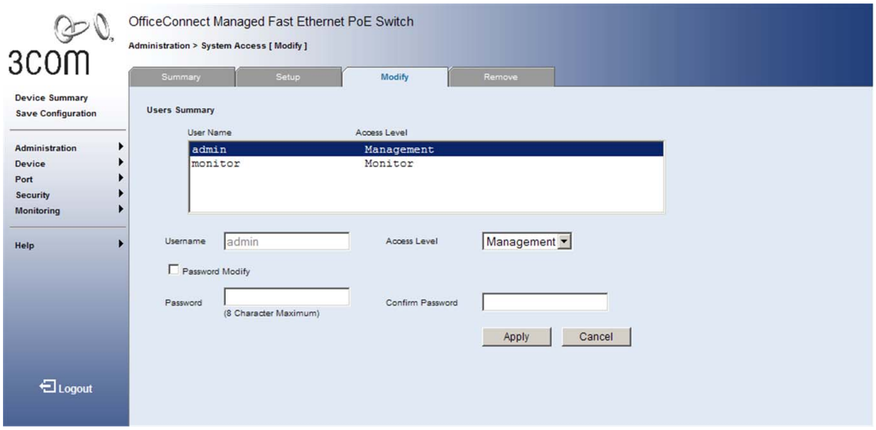
2 Enter requisite information in the text field.

3 Click Apply . The IP information is configured, and the device is updated.

Modifying Configuration Information

1 Click **Administration** > **System Access** > **Modify**. The *System Access Modify Page* opens:

Figure 14 System Access Modify Page



Users Summary

User Name	Access Level
admin	Management
monitor	Monitor

Username: admin
Access Level: Management
□ Password Modify
Password: (8 Character Maximum)
Confirm Password:

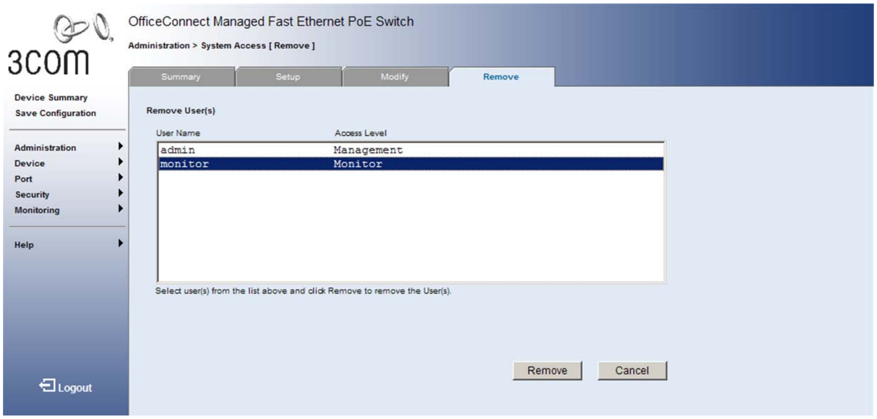
2 Modify the fields.

3 Click Apply. The access fields are modified.

Removing Configuration Information

1 Click **Administration > System Access > Remove**. The *System Access Remove Page* opens:

Figure 15 System Access Remove Page



Remove User(s)

User Name	Access Level
admin	Management
monitor	Monitor

Select user(s) from the list above and click Remove to remove the User(s).

2 Select the user account to be deleted.

3 Click Remove. The user account is deleted, and the device is updated.

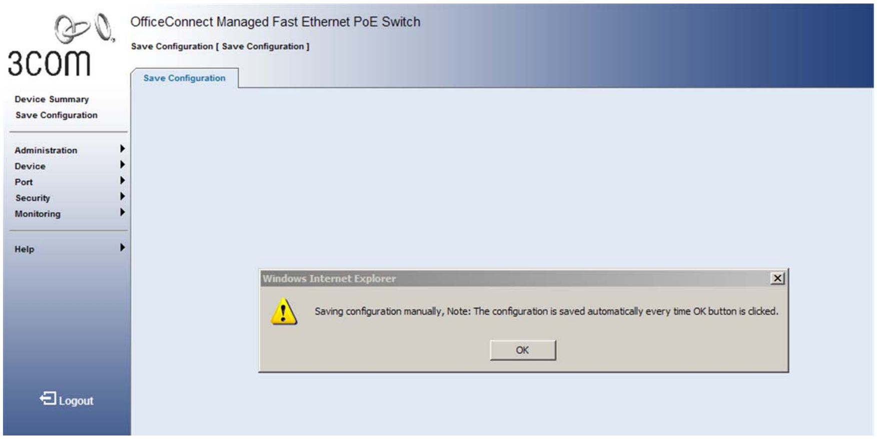
Saving the Configuration

Configuration changes are saved to the device's flash memory every time the OK button is clicked. The Save Configuration tab also allows the latest configuration to be saved to the flash memory.

To save the device configuration:

1 Click **Save Configuration**. The *Save Configuration Page* opens:

Figure 16 Save Configuration Page



Windows Internet Explorer

Saving configuration manually, Note: The configuration is saved automatically every time OK button is clicked.

A message appears: *Saving configuration manually. Note: The configuration is saved automatically every time OK button is clicked. The operation will save your configuration. Do you wish to continue?*

2 Click OK. The configuration is saved.

Resetting the Device

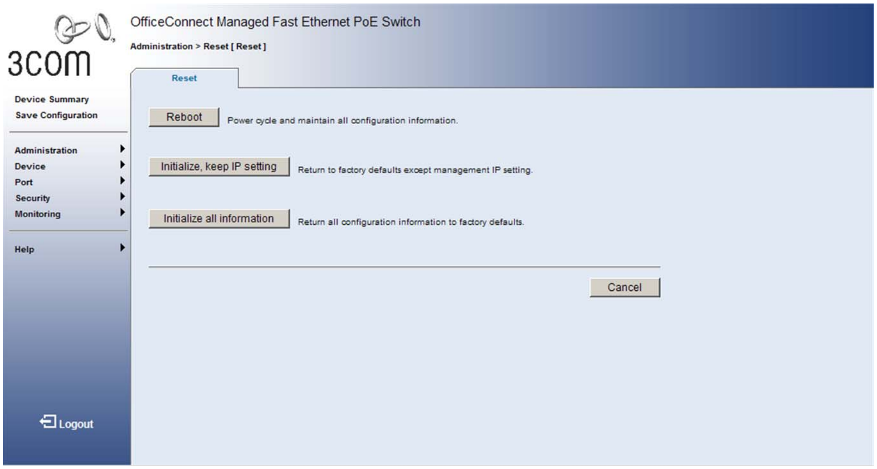
The *Reset Page* enables resetting the device from a remote location.

To prevent the current configuration from being lost, use the *Save Configuration Page* to save all user-defined changes to the flash memory before resetting the device.

To reset the device:

1 Click **Administration > Reset**. The *Reset Page* opens:

Figure 17 Reset Page


3com
OfficeConnect Managed Fast Ethernet PoE Switch
Administration > Reset [Reset]
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Reset
Reboot
Initialize, keep IP setting
Initialize all information
Cancel

Reboot — Power cycle and maintain all configuration information.

Initialize, keep IP setting — Return to factory defaults except management IP setting.

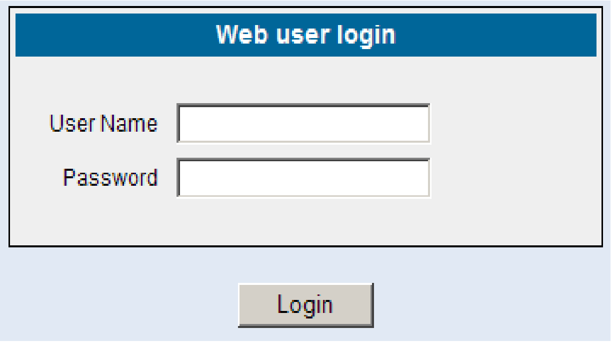
Initialize all information — Return all configuration information to factory defaults.

2 Click Reboot. A confirmation message is displayed.

3 Click OK. Another message is displayed indicating that the device will reboot in 15 seconds.

4 Click OK again. The device is reset, and a prompt for a user name and password is displayed.

Figure 18 User Name and Password Page



5 Enter a user name and password to reconnect to the web interface.

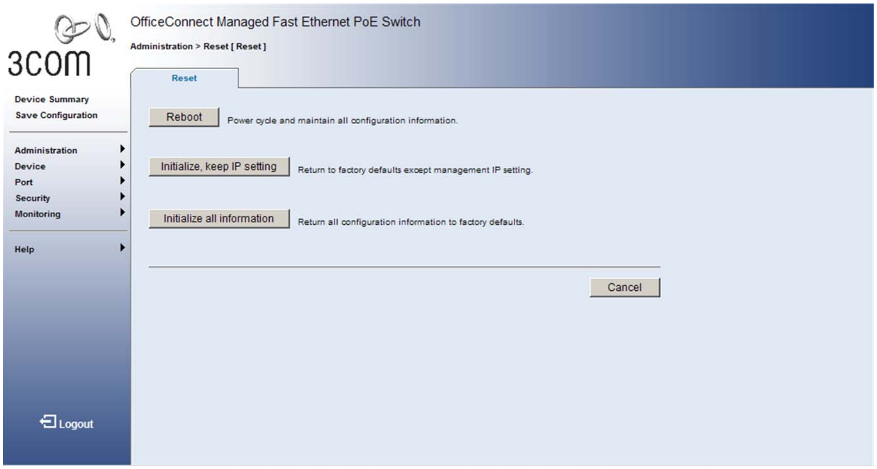
Restoring Factory Defaults

The Restore option appears on the *Reset Page*. The Restore option restores device factory defaults.

To restore the device:

1 Click **Administration > Reset**. The *Reset Page* opens:

Figure 19 Reset Page


3com
OfficeConnect Managed Fast Ethernet PoE Switch
Administration > Reset [Reset]
Reset
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Reboot
Initialize, keep IP setting
Initialize all information
Cancel

Power cycle and maintain all configuration information.

Return to factory defaults except management IP setting.

Return all configuration information to factory defaults.

The *Reset Page* contains the following fields:

- **Initialize, keep IP Setting** — Resets the device with the factory default settings, but maintains the current IP Address.
- **Initialize all information** — Resets the device with the factory default settings, including the IP Address.

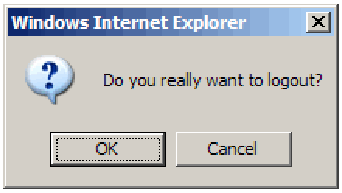
2 Click Initialize, keep IP setting or Initialize all information. The system is restored to factory defaults.

Logging Off the Device

To log off the device:

1 Click Logout. The *Logout Page* opens.

2 The following message appears:



Windows Internet Explorer

Do you really want to logout?

3 Click OK. The *3Com Web Interface Home Page* closes.

3 VIEWING BASIC SETTINGS

This section contains information for viewing basic settings. The *3Com Web Interface Home Page* presents a device summary section that provides the system administrator with the option to view essential information required for setting up and maintaining device settings.

The *Device Summary Section* contains the following views:

- Viewing Device Settings
- Configuring the Polling Interval
- Viewing Color Keys

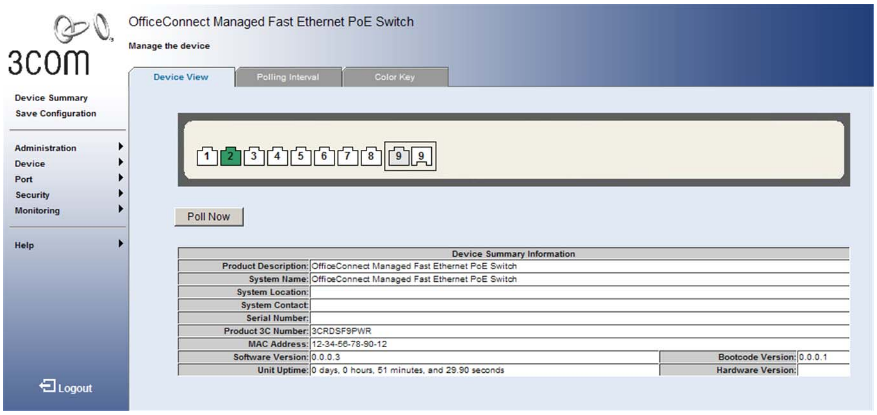
Viewing Device Settings

The *Device Summary Page* displays parameters for viewing general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System Up Time, and MAC addresses, and both software, boot, and hardware versions.

To view the Device Summary Settings:

1 Click **Device Summary**. The *Device Summary Page* opens:

Figure 20 Device Summary Page



Device Summary Information			
Product Description:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Name:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Location:			
System Contact:			
Serial Number:			
Product 3C Number:	3CRDSF9PWR		
MAC Address:	12-34-56-78-90-12		
Software Version:	0.0.0.3	Bootcode Version:	0.0.0.1
Unit Uptime:	0 days, 0 hours, 51 minutes, and 29.90 seconds	Hardware Version:	

The *Device Summary Page* contains the following fields:

- **Poll Now** — Enables polling the ports for port information including speed, utilization and port status.
- **Product Description** — Displays the device name.
- **System Name** — Defines the user-defined device name. The field length is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field length is 0-160 characters.
- **Serial Number** — Displays the device serial number.
- **Product 3C Number** — Displays the 3Com device 3C number.
- **MAC Address** — Displays the device MAC address.
- **Software Version** — Displays the installed software version number.

- **Unit Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.
- **Boot Code Version** — Displays the current boot version running on the device.
- **Hardware Version** — Displays the current hardware version of the device.

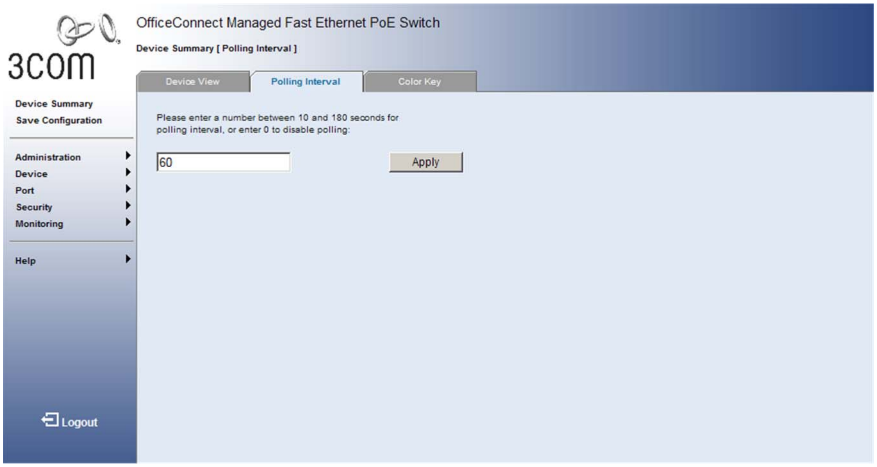
Configuring the Polling Interval

The *Polling Interval Page* displays the interval at which information on the Web management pages is refreshed.

To configure the polling interval:

1 Click **Device Summary > Polling Interval**. The *Polling Interval Page* opens:

Figure 21 Polling Interval Page



Please enter a number between 10 and 180 seconds for polling interval, or enter 0 to disable polling:

60

The *Polling Interval Page* contains the following fields:

- Polling Interval — Displays the current setting for the polling interval. The range for this field is 10-180 seconds, and the default is 60 seconds. This field can also be set to 0 seconds to disable polling.

2 Define the polling interval.

3 Click Apply. The polling interval is set, and the device is updated.

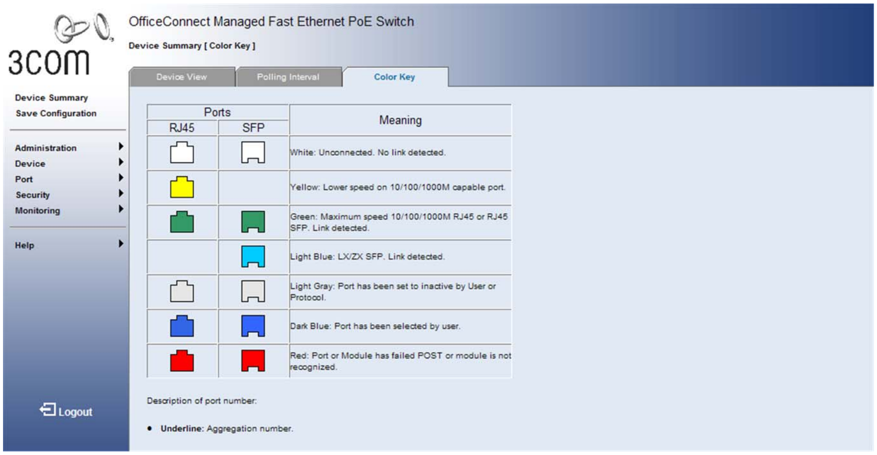
Viewing Color Keys

The *Color Key Page* provides information regarding the RJ45 or SFP port status on the device. The various colors key indicate the port status, speed and link of a selected port.

To view color keys:

1 Click **Device Summary > Color Key**. The *Color Key Page* opens:

Figure 22 Color Key Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device Summary [Color Key]

Ports		Meaning
RJ45	SFP	
□	□	White: Unconnected. No link detected.
🟨		Yellow: Lower speed on 10/100/1000M capable port.
🟩	🟩	Green: Maximum speed 10/100/1000M RJ45 or RJ45 SFP. Link detected.
	🟦	Light Blue: LX/ZX SFP. Link detected.
⬜	⬜	Light Gray: Port has been set to inactive by User or Protocol.
🟦	🟦	Dark Blue: Port has been selected by user.
🟥	🟥	Red: Port or Module has failed POST or module is not recognized.

Description of port number:

- **Underline:** Aggregation number.

The *Color Key Page* contains the following fields:

- **RJ45** — Displays the port status of the *Registered Jack 45* (RJ45) connections which are the physical interface used for terminating twisted pair type cable.
- **SFP** — Displays the port status of the *Small Form Factor Pluggable* (SFP) optical transmitter modules that combine transmitter and receiver functions.

The table includes the color and the port status:

- *White* — Unconnected. No link detected.
- *Yellow* — Lower speed on 10/100/1000M port.
- *Green* — Maximum speed 10/100/1000M RJ45 or SFP. Indicates that a link was detected.
- *Light Blue* — SX/LX/BX SFP. Indicates that a link was detected.
- *Light Gray* — Port has been set to inactive by User or Protocol.
- *Dark Blue* — Port has been selected by user.
- *Red* — Port or Transceiver has failed POST or Transceivers not recognized.

4 MANAGING DEVICE SECURITY

The Management Security section provides information for configuring system access, defining RADIUS authentication, port-based authentication, and access control lists.

This section includes the following topics:

- Configuring System Access
- Defining RADIUS Clients
- Defining Port-Based Authentication (802.1X)
- Defining Local Database Authentication
- Encrypting Connection to the Web Interface (HTTPS)
- Using the Secure Shell Protocol (SSH)
- Defining Access Control Lists
- Using Broadcast Storm Control

Configuring System Access

Network administrators can define users, passwords, and access levels for users using the System Access Interface. The Multi-Session web feature is enabled on device and allows 16 users to be created and access the switch concurrently. Access levels provide read or read/write permissions to users for configuring the switch. Login information is managed in the local database. A unique password is required of each user. Two access levels exist on the 3Com Web Interface:

- **Management access level** — Provides the user with read/write access. There is always one management level user configured for the switch. The factory default user name is: *admin* with no password.
- **Monitor access level** — Provides the user with read-only system access.

This section contains the following topics:

- Viewing System Access Settings
- Defining System Access
- Modifying System Access
- Removing System Access

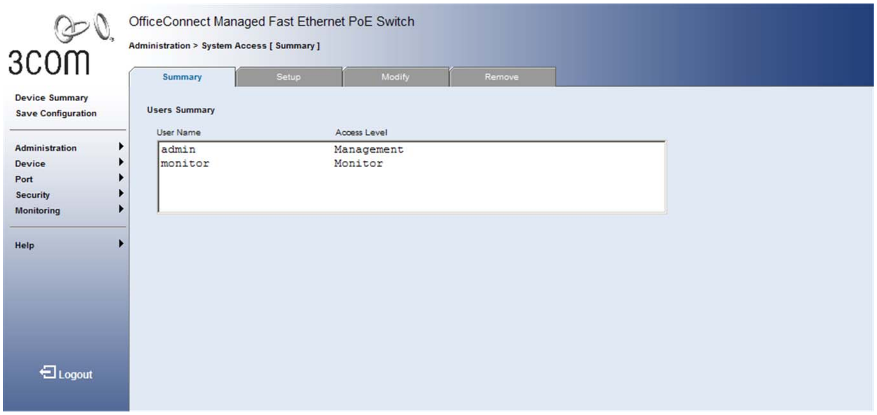
Viewing System Access Settings

The *System Access Summary Page* displays the current users and access levels defined on the device.

To view System Access settings:

1 Click **Administration > System Access > Summary**. The *System Access Summary Page* opens:

Figure 23 System Access Summary Page



Users Summary

User Name	Access Level
admin	Management
monitor	Monitor

The *System Access Summary Page* contains the following fields:

- **User Name** — Displays the user names. The possible predefined field values are:
  - *admin* — Displays the predefined administrative user name.
  - *monitor* — Displays the predefined monitor user name.
- **Access Level** — Displays the user access level. The lowest user access level is *Monitor* and the highest is *Management*.
  - *Management* — Provides the user with read and write access rights.
  - *Monitor* — Provides the user with read access rights.

Defining System Access

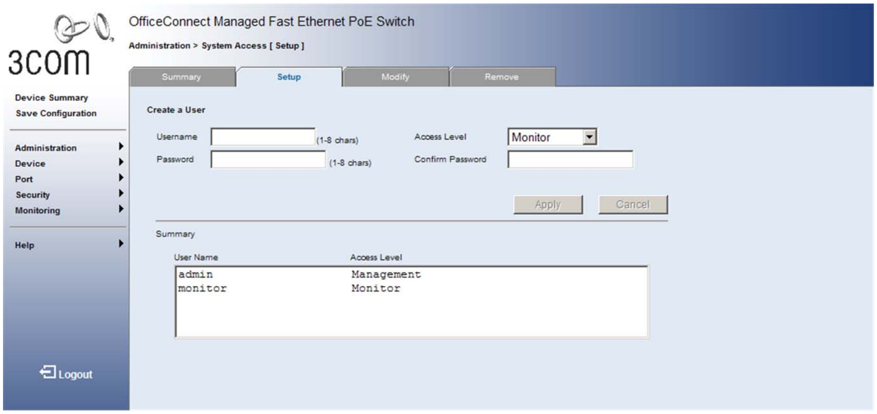
The *System Access Setup Page* allows network administrators to define users, passwords, and access levels for users using the System Access Interface.

Monitor users have no access to this page.

To define System Access:

1 Click **Administration > System Access > Setup**. The *System Access Setup Page* opens:

Figure 24 System Access Setup Page



Access Level: Monitor

Summary

User Name	Access Level
admin	Management
monitor	Monitor

The *System Access Setup Page* contains the following fields:

- **User Name** — Defines the user name.
- **Access Level** — Defines the user access level. The lowest user access level is *Monitor* and the highest is *Management*.
  - *Management* — Provides users with read and write access rights.
  - *Monitor* — Provides users with read access rights.
- **Password** — Defines the user password. User passwords can contain up to 10 characters.
- **Confirm Password** — Verifies the password.

2 Define the fields.

3 Click Apply. The user is created, and the device is updated.

Modifying System Access

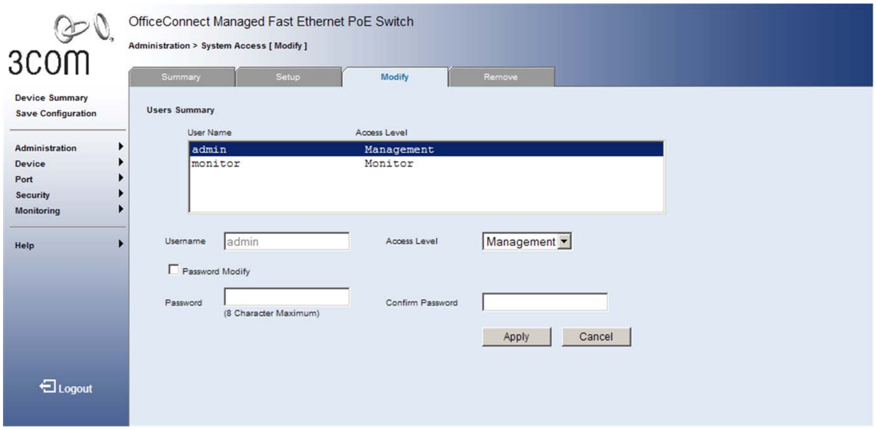
The *System Access Modify Page* allows network administrators to modify users, passwords, and access levels for users using the System Access Interface.

Monitor users have no access to this page.

To modify System Access:

1 Click **Administration > System Access > Modify**. The *System Access Modify Page* opens:

Figure 25 System Access Modify Page



Users Summary

User Name	Access Level
admin	Management
monitor	Monitor

Username: admin

Access Level: Management

□ Password Modify

Password: (8 Character Maximum)

Confirm Password:

The *System Access Modify Page* contains the following fields:

- **User Name** — Displays the user name.
- **Access Level** — Specifies the user access level. The lowest user access level is *Monitoring* and the highest is *Management*.
  - *Management* — Provides users with read and write access rights.
  - *Monitor* — Provides users with read access rights.
- **Password Modify** — Enables modifying a password for an existing user.
- **Password** — Defines the local user password. Local user passwords can contain up to 10 characters.
- **Confirm Password** — Verifies the password.

2 Select a *User Name* whose settings are to be modified.

3 Modify the fields.

4 Click Apply. The user settings are modified, and the device is updated.

Removing System Access

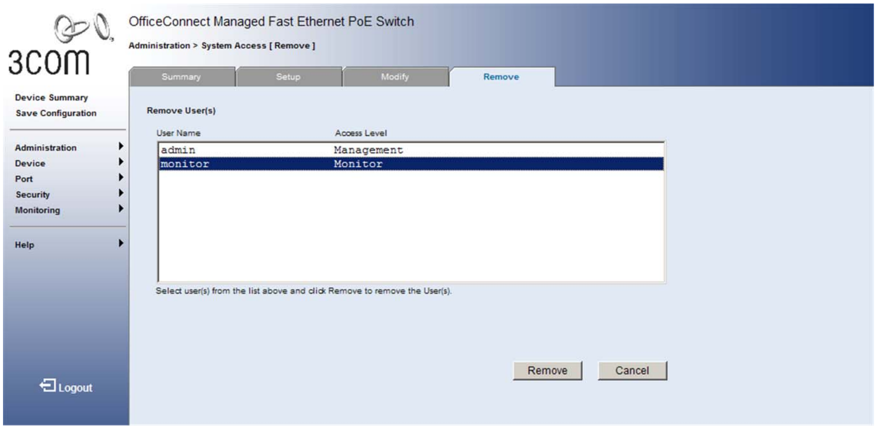
The *System Access Remove Page* allows network administrators to remove users from the System Access Interface.

Monitor users have no access to this page.

To remove users:

1 Click **Administration > System Access > Remove**. The *System Access Remove Page* opens:

Figure 26 System Access Remove Page



User Name	Access Level
admin	Management
monitor	Monitor

Select user(s) from the list above and click Remove to remove the User(s).

The *System Access Remove Page* contains the following fields:

Remove User(s) — Users to be removed can be selected from the list below.

- **User Name** — Displays the user name.
- **Access Level** — Displays the user access level. The lowest user access level is *Monitoring* and the highest is *Management*.
  - *Management* — Provides users with read and write access rights.
  - *Monitoring* — Provides users with read access rights.

2 Select the *Users* to be deleted.

The last user with management access may not be deleted.

3 Click Remove. The *Users* are deleted, and the device is updated.

Defining RADIUS Clients

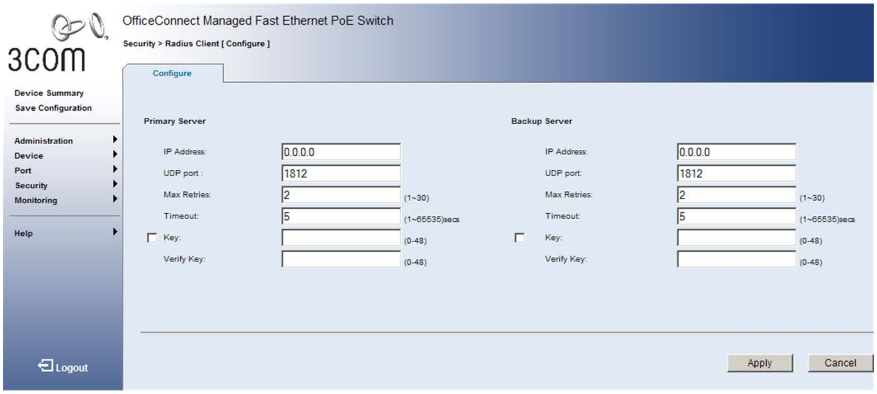
Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for 802.1X.

Monitor users have no access to this page.

To configure the RADIUS client:

1 Click **Security > RADIUS Client > Configure**. The *RADIUS Client Configure Page* opens:

Figure 27 RADIUS Client Configure Page



Primary Server

IP Address: 0.0.0.0
UDP port : 1812
Max Retries: 2 (1~30)
Timeout: 5 (1~65535)secs
□ Key: (0-48)
Verify Key: (0-48)

Backup Server

IP Address: 0.0.0.0
UDP port: 1812
Max Retries: 2 (1~30)
Timeout: 5 (1~65535)secs
□ Key: (0-48)
Verify Key: (0-48)

The *RADIUS Client Configure Page* contains the following fields:

- **Primary Server** — Defines the RADIUS Primary Server authentication fields.
- **Backup Server** — Defines the RADIUS Backup Server authentication fields.
- **IP Address** — Defines the RADIUS Server IP address.
- **UDP Port** — Defines the authentication port. The authentication port is used to verify RADIUS server authentication. The authentication port default is *1812*.
- **Max Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are *1-30*. The default value is *2*.
- **Timeout** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or

switching to the next server. Possible field values are *1-65535*. The default value is *5*.

- **Key** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the switch and the RADIUS server. This key must match the RADIUS encryption. The range is 0-48 characters. Do not use blank spaces.
- **Verify Key** — Verifies the key.

2 Define the fields.

3 Click Apply. The RADIUS client is enabled, and the system is updated.

Defining Port-Based Authentication (802.1X)

Port-based authentication authenticates 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 RADIUS server using the *Extensible Authentication Protocol* (EAP). Port-based authentication includes:

- **Authenticators** — Specifies the device port which is authenticated before permitting system access.
- **Supplicants** — Specifies the host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port-based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

This section includes the following topics:

- Viewing 802.1X Authentication
- Defining 802.1X Authentication

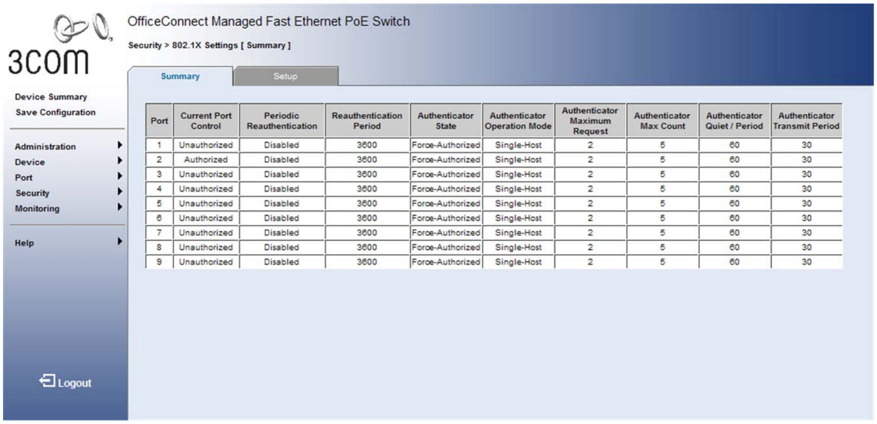
Viewing 802.1X Authentication

The *802.1X Summary Page* allows the network administrator to view port-based authentication settings.

To view Port-based Authentication:

1 Click **Security > 802.1X > Summary**. The *802.1X Summary Page* opens:

Figure 28 802.1X Summary Page



Security > 802.1X Settings [Summary]

Port	Current Port Control	Periodic Reauthentication	Reauthentication Period	Authenticator State	Authenticator Operation Mode	Authenticator Maximum Request	Authenticator Max Count	Authenticator Quiet / Period	Authenticator Transmit Period
1	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
2	Authorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
3	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
4	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
5	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
6	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
7	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
8	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30
9	Unauthorized	Disabled	3600	Force-Authorized	Single-Host	2	5	60	30

The *802.1X Summary Page* contains the following fields:

- **Port** — Displays a list of interfaces.
- **Current Port Control** — Displays the current port authorization state.
- **Periodic Reauthentication** — Reauthentication can be used to detect if a new device is plugged into a switch port. If enabled, the client will be reauthenticated after the interval specified by the Reauthentication Period.
  - *Enabled* — Periodic reauthentication is enabled on the port.
  - *Disabled* — Periodic reauthentication is disabled on the port. This is the default.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is *3600* seconds.
- **Authenticator State** — Displays the current authenticator state.
  - *Auto* — Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

  - *Force-Authorized* — Indicates that any client has full access to the port, even if it does not have 802.1X credentials or support 802.1X authorization.
  - *Force-Unauthorized* — Indicates that no client has access to the port, even if it has 802.1X credentials and supports 802.1X authorization.
- **Authenticator Operation Mode** — Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port.
  - *Multi-Host* — Allows multiple hosts to connect to this port.
  - *Single-Host* — Allows only a single host to connect to this port. This is the default.
- **Authenticator Maximum Request** — Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. The field default is *2*.
- **Authenticator Max Count** — The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. The field default is *5*.
- **Authenticator Quiet Period** — Sets the time that a switch port waits after the Authenticator Max Count has been exceeded before attempting to acquire a new client. The field default is *60* seconds.
- **Authenticator Transmit Period** — Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. The field default is *30* seconds.

Defining 802.1X Authentication

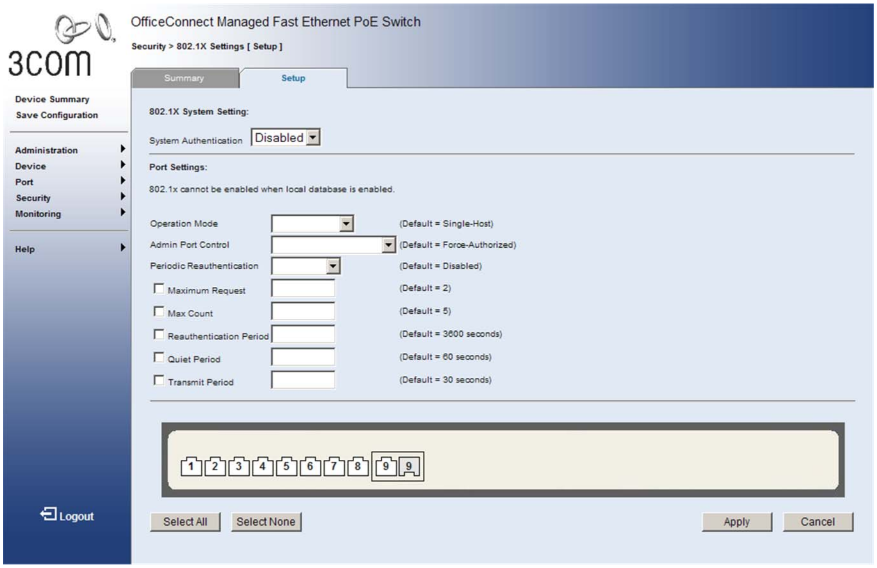
The *802.1X Setup Page* contains information for configuring 802.1X global settings on the device and defining specific 802.1X settings for each port.

Monitor users have no access to this page.

To configure 802.1X Settings:

1 Click **Security > 802.1X > Setup**. The *802.1X Setup Page* opens:

Figure 29 802.1X Setup Page



802.1X System Setting:

System Authentication: Disabled

Port Settings:

802.1x cannot be enabled when local database is enabled.

Operation Mode (Default = Single-Host)
Admin Port Control (Default = Force-Authorized)
Periodic Reauthentication (Default = Disabled)
□ Maximum Request (Default = 2)
□ Max Count (Default = 5)
□ Reauthentication Period (Default = 3600 seconds)
□ Quiet Period (Default = 60 seconds)
□ Transmit Period (Default = 30 seconds)

The *802.1X Setup Page* contains the following fields:

802.1X System Setting

- **System Authentication** — Specifies if Port Authentication is enabled on the device. The possible field values are:
  - *Enabled* — Enables port-based authentication on the device.
  - *Disabled* — Disables port-based authentication on the device. This is the default.

Port Settings

- **Operation Mode** — Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port.
  - *Multi-Host* — Allows multiple hosts to connect to this port.

    - *Single-Host* — Allows only a single host to connect to this port. This is the default.
- **Admin Port Control** — Specifies the admin port authorization state.
    - *Auto* — Enables port based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
    - *Force-Authorized* — Places the interface into an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port based authentication.
    - *Force-Unauthorized* — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Periodic Reauthentication** — Enables periodic reauthentication on the port.
    - *Enabled* — Enables periodic reauthentication on the port.
    - *Disabled* — Disables periodic reauthentication on the port.
- **Maximum Request** — Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. The field default is *2*, the range is *1-10*.
- **Max Count** — The maximum number of hosts that can connect to a port when Multi-Host operation mode is selected. The field default is *5,* the range is *1-1024*.
- **Reauthentication Period** — Defines the time span (in seconds) in which the selected port is reauthenticated. The field default is *3600* seconds, the range is *1-65535*.
- **Quiet Period** — Sets the time that a switch port waits after the Authenticator Max Count has been exceeded before attempting to acquire a new client. The field default is *60* seconds, the range is *1-65535* seconds.
- **Transmit Period** — Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. The field default is *30* seconds, the range is *1-65535* seconds.

2 Define the fields.

3 Click Apply. The 802.1X Settings are enabled, and the device is updated.

Defining Local Database Authentication

Local database authentication allows stations to authenticate and access the network in situations where 802.1X authentication is infeasible or impractical. The local database authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication. Once authentication is successful, the user is forwarded on to the originally requested web page.

This section includes the following topics:

- Configuring Local Database Authentication
- Viewing Port Settings
- Configuring Port Settings
- Viewing User Listing
- Creating User Entries
- Modifying User Entries
- Removing User Entries

Configuring Local Database Authentication

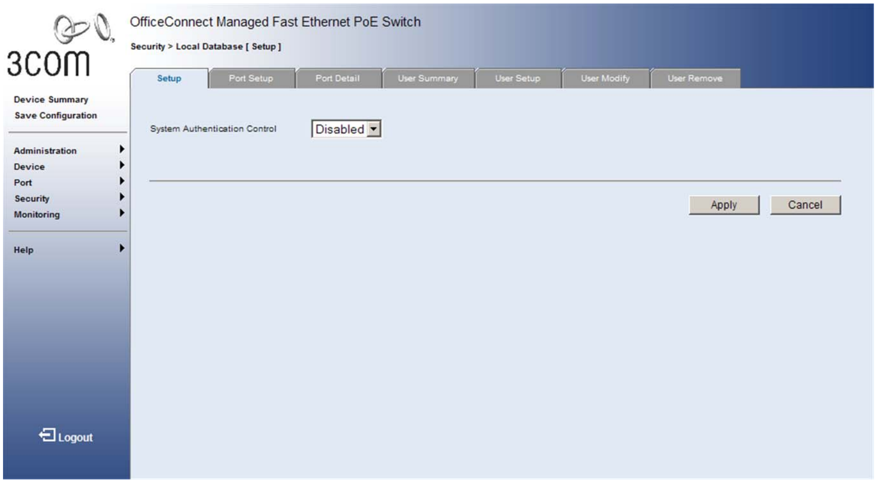
The *Local Database Setup Page* allows the network administrator to globally enable or disable local-database authentication for the switch.

Monitor users have no access to this page.

To configure Local Database Settings:

1 Click **Port > Local Database > Setup**. The *Local Database Setup Page* opens:

Figure 30 Local Database Setup Page



System Authentication Control: Disabled

The *Local Database Setup Page* contains the following fields:

- **System Authentication Control** — Configures local-database authentication globally for the switch. The possible field values are:
  - *Enabled* — Enables local database authentication on the device.
  - *Disabled* — Disables local database authentication on the device. This is the default.

2 Define the fields.

3 Click Apply. The Local Database Settings are enabled, and the device is updated.

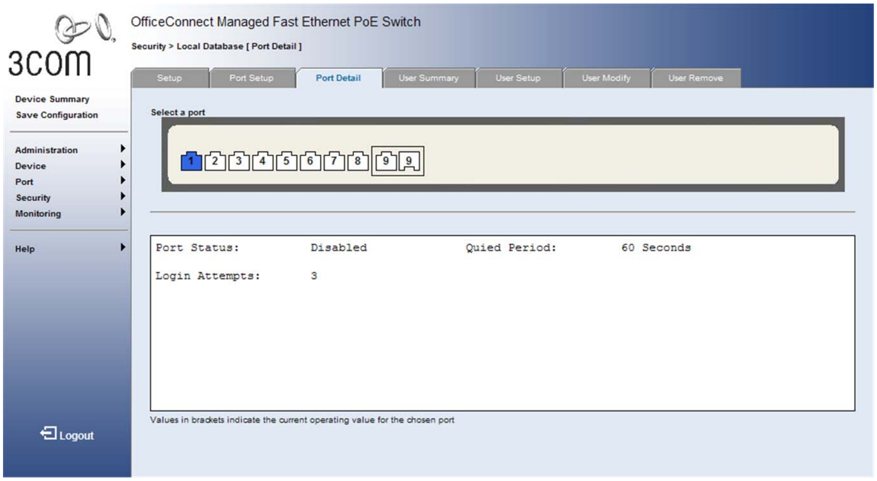
Viewing Port Settings

The *Local Database Port Detail Page* displays local-database protocol settings for the selected port.

To display protocol settings for Local Database Authentication:

1 Click **Port > Local Database > Port Detail**. The *Local Database Port Detail Page* opens:

Figure 31 Local Database Port Detail Page



```
Port Status:          Disabled              Quied Period:          60 Seconds

Login Attempts:       3
```

Values in brackets indicate the current operating value for the chosen port

The *Local Database Port Detail Page* contains the following fields:

- **Port Status** — Displays the administrative status of local-database authentication for a port. The possible field values are:
  - *Enabled* — Enables local database authentication on the device.
  - *Disabled* — Disables local database authentication on the device.
- **Quiet Period** — Displays the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt local-database authentication again.
- **Login Attempts** — Displays the limit on failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires.

Configuring Port Settings

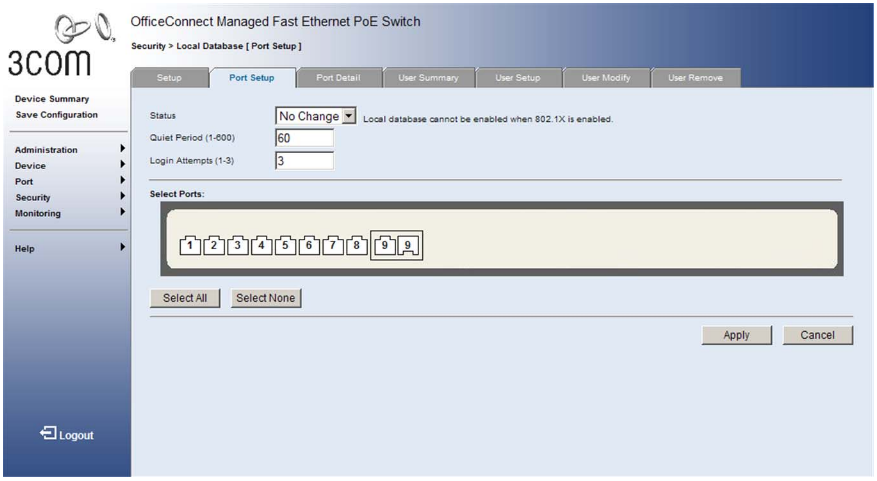
The *Local Database Port Setup Page* allows the network administrator to configure local-database protocol settings for the selected port.

Monitor users have no access to this page.

To display protocol settings for Local Database Authentication:

1 Click **Port > Local Database > Port Setup**. The *Local Database Port Setup Page* opens:

Figure 32 Local Database Port Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Security > Local Database [Port Setup]

Status: No Change — Local database cannot be enabled when 802.1X is enabled.

Quiet Period (1-600): 60

Login Attempts (1-3): 3

The *Local Database Port Setup Page* contains the following fields:

- **Status** — Configures the administrative status of local-database authentication for a port. The possible field values are:
  - *Enabled* — Enables local database authentication on the device.
  - *Disabled* — Disables local database authentication on the device. This is the default.
  - *No Change* — Retains the current port status.
- **Quid Period** — Displays the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt local-database authentication again. The field range is *1-600* seconds, and the default is *60* seconds.
- **Login Attempts** — Displays the limit on failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. The field range is *1-3* attempts, and the default is *3* attempts.

2 Define the fields.

3 Select the ports to which these settings will be applied.

4 Click Apply. The Local Database Settings are enabled, and the device is updated.

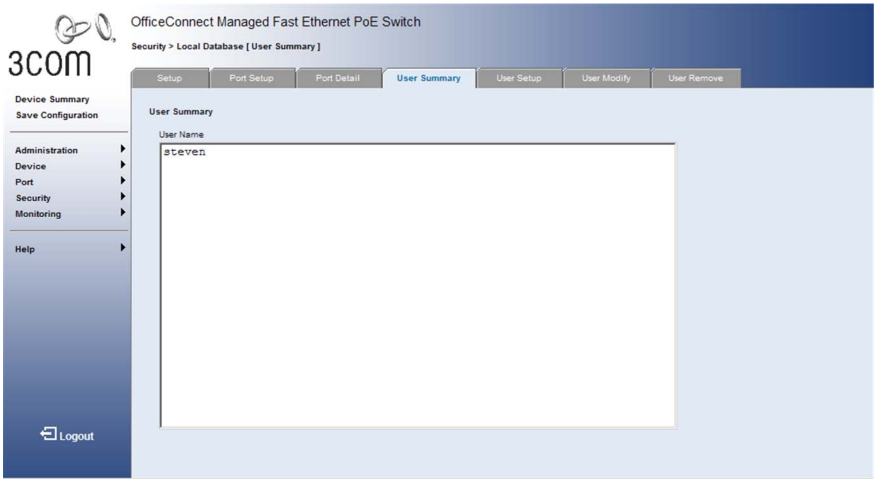
Viewing User Listing

The *Local Database User Summary Page* displays user names stored in the local database.

To display the users stored in the Local Database:

1 Click **Port > Local Database > User Summary**. The *Local Database User Summary Page* opens:

Figure 33 Local Database User Summary Page



User Summary

User Name

steven

The *Local Database User Summary Page* contains the following fields:

- **User Name** — The name of users stored in the local database.

Creating User Entries

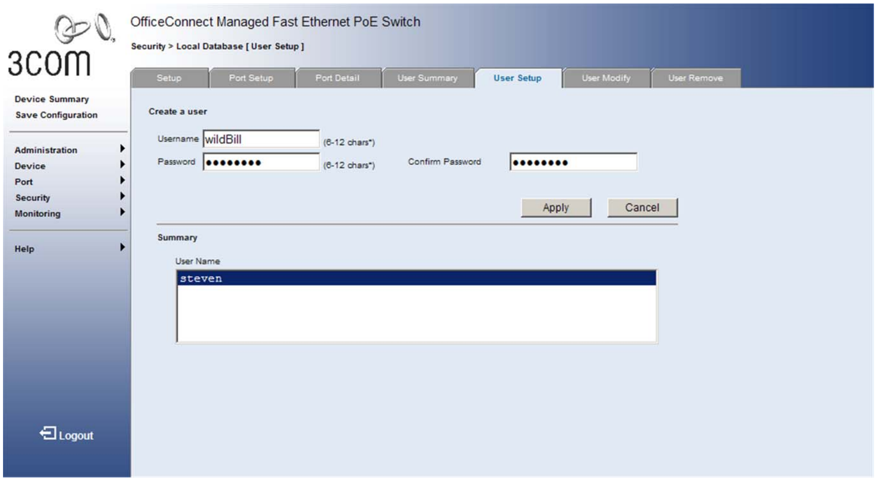
The *Local Database User Setup Page* allows the network administrator to configure user name/password entries in the local database.

Monitor users have no access to this page.

To create user entries in the Local Database:

1 Click **Port > Local Database > User Setup**. The *Local Database User Setup Page* opens:

Figure 34 Local Database User Setup Page



Create a user

Username wildBill (6-12 chars*)

Password •••••••• (6-12 chars*) Confirm Password ••••••••

Summary

User Name

steven

The *Local Database User Setup Page* contains the following fields:

- **Create a User**
  - **User Name** — The name of a user to be authorized restricted network access through local database authentication. String length is 6-12 characters (case sensitive), and the maximum number of users is 250.
  - **Password** — The authentication password for the corresponding user. String length is 6-12 characters (case sensitive).
  - **Confirm Password** — Verifies the password.
- **Summary**
  - **User Name** — Displays the users stored in the local database.

2 Define the fields for a user.

3 Click Apply. The entry is added to the Local Database, and the device is updated.

Modifying User Entries

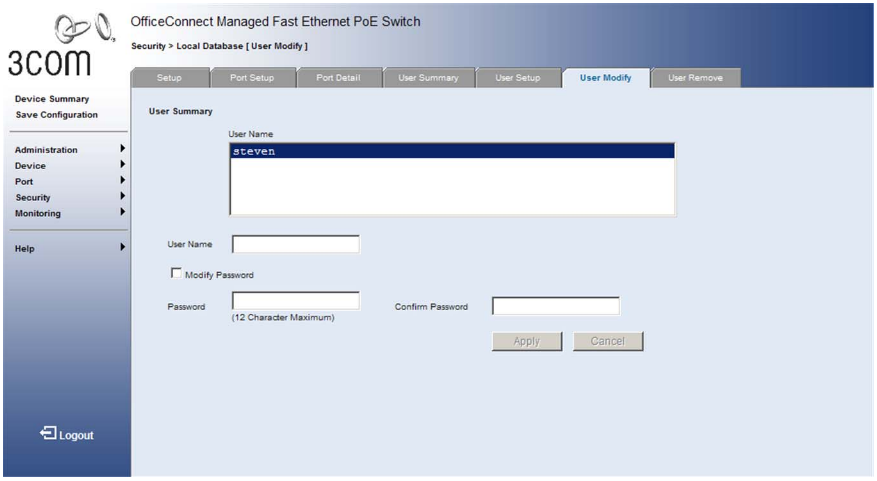
The *Local Database User Modify Page* allows the network administrator to change the password for users stored in the local database.

Monitor users have no access to this page.

To modify the password for user entries in the Local Database:

1. Click **Port > Local Database > Modify**. The *Local Database User Modify Page* opens:

Figure 35 Local Database User Modify Page



The *Local Database User Modify Page* contains the following fields:

- **User Name** — The name of a user stored in the local database.
- **Password Modify** — Mark this box to modify the password for the selected user.
  - **Password** — The authentication password for the corresponding user. String length is 6-12 characters (case sensitive).
  - **Confirm Password** — Verifies the password.

2. Select a user from the User Summary list.
3. Mark the Password Modify box.
4. Enter a new password and then confirm it.
5. Click Apply. The user entry is updated in the Local Database, and the device is updated.

Removing User Entries

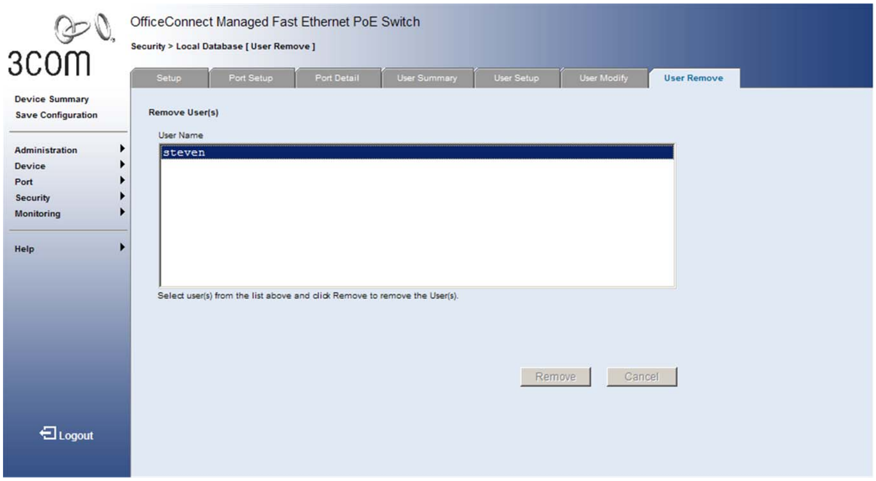
The *Local Database User Remove Page* allows the network administrator to remove user entries stored in the local database.

Monitor users have no access to this page.

To remove a user entry from the Local Database:

1 Click **Port > Local Database > Remove**. The *Local Database User Remove Page* opens:

Figure 36 Local Database User Remove Page



steven

Select user(s) from the list above and click Remove to remove the User(s).

The *Local Database User Remove Page* contains the following fields:

- **User Name** — The name of a user stored in the local database.

2 Select a user from the list.

3 Click Remove . The user entry is removed from the Local Database, and the device is updated.

Encrypting Connection to the Web Interface (HTTPS)

HTTPS allows secure access to the Web interface of the switch. If you administer your switch remotely or over an insecure network, the switch can encrypt all HTTP traffic to and from the Web interface using the Secure Sockets Layer (SSL) of HTTP. If your network traffic is intercepted, no passwords or configuration information will be visible in the data.

To use HTTPS you need the following:

- A browser that supports SSL
- A digital certificate installed on the switch

The switch ships with a default certificate installed. This certificate has not been validated by a Certifying Authority and your browser may warn you that the certificate has not been certified. Using a properly validated certificate provides a higher level of security than the default certificate.

You can securely browse your switch by using the HTTPS (HTTP over SSL) protocol. To access the Web interface securely, enter the following into your browser:

```
https://xxx.xxx.xxx.xxx/
```

where xxx.xxx.xxx.xxx is the IP address of your switch.

Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same TCP port.

If you enable HTTPS, you must indicate this in the URL that you specify in your browser and specify the port number if not using the default value: **https**://*device*[:*port_number*]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server’s digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.

The client and server establish a secure encrypted connection.
A padlock icon should appear in the status bar for Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

Table 9 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

Configuring HTTPS

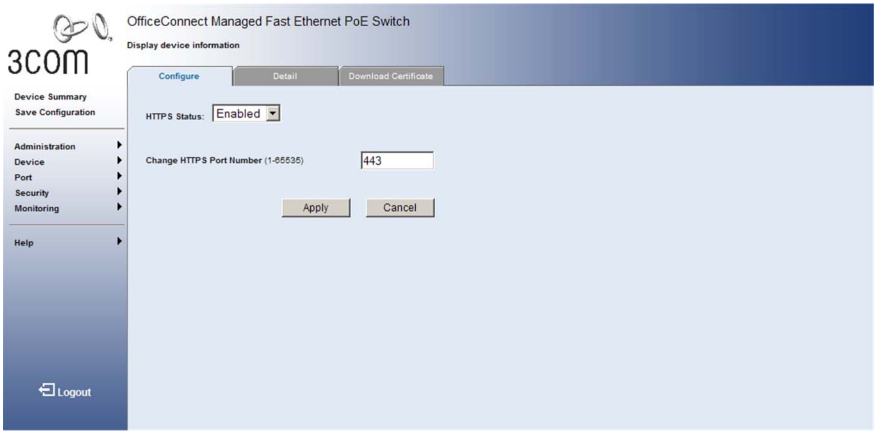
The *HTTPS Configure Page* allows network administrators to enable or disable HTTPS and set the TCP port number for this service.

Monitor users have no access to this page.

To configure HTTPS settings:

1 Click **Security > HTTPS Settings > Configure**. The *HTTPS Configure Page* opens:

Figure 37 HTTPS Configure Page



OfficeConnect Managed Fast Ethernet PoE Switch

Display device information

HTTPS Status: Enabled

Change HTTPS Port Number (1-65535) 443

The *HTTPS Configure Page* contains the following fields:

- HTTPS Status — Specifies if HTTPS is enabled on the device. The possible predefined field values are:
  - *Enabled* — HTTPS is enabled on the device. This is the default.

  - *Disabled* — HTTPS is disabled on the device.
- Change HTTPS Port Number — Specifies the TCP port to be used for HTTPS. The default value is *443*, and the range is *1-65535*.

You cannot configure the HTTP and HTTPS servers to use the same port.

If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL in this format:

https://*device*:*port_number*

2 Define the fields.

3 Click Apply . The HTTPS settings are updated.

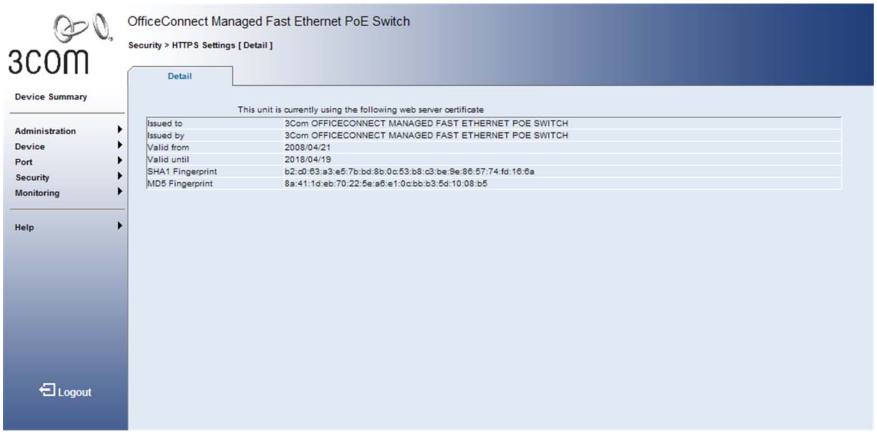
Displaying the Web Server Certificate

The *HTTPS Detail Page* allows users to display detailed information about the web server certificate.

To view information about the digital certificate:

1 Click **Security > HTTPS Settings > Detail**. The *HTTPS Detail Page* opens:

Figure 38 HTTPS Detail Page



OfficeConnect Managed Fast Ethernet PoE Switch
Security > HTTPS Settings [Detail]
Detail
Device Summary
Administration
Device
Port
Security
Monitoring
Help
Logout

This unit is currently using the following web server certificate

Issued to	3Com OFFICECONNECT MANAGED FAST ETHERNET POE SWITCH
Issued by	3Com OFFICECONNECT MANAGED FAST ETHERNET POE SWITCH
Valid from	2008/04/21
Valid until	2018/04/19
SHA1 Fingerprint	b2:c0:63:a3:e5:7b:bd:8b:0c:53:b8:c3:be:9e:86:57:74:fd:16:6a
MD5 Fingerprint	8a:41:1d:eb:70:22:5e:a6:e1:0c:bb:b3:5d:10:08:b5

The *HTTPS Detail Page* contains the following fields:

- Issued to — Shows the registered user of this certificate.
- Issued by — Shows the certification authority that issued this certificate.
- Valid from/until — Shows the validity period for this certificate.
- SHA1 Fingerprint — Hash sting used to encrypt communications.
- MD5 Fingerprint — Hash sting used to encrypt communications.

Changing the Digital Certificate

The switch ships with a default certificate. However, this certificate has not been validated by a Certifying Authority. Using a properly validated certificate provides a higher level of security than the default certificate.

To access your switch using HTTPS, you need a digital certificate which identifies it. The switch uses certificates that adhere to the X.509 standard.

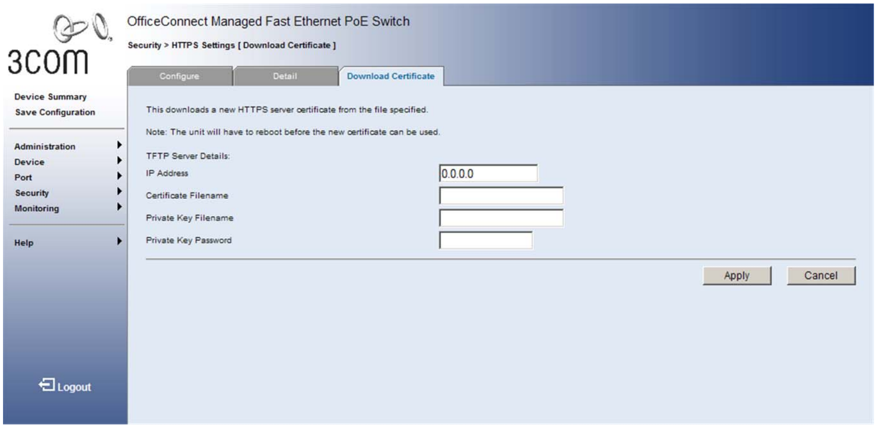
If you have the software to generate an X.509 certificate, you can self-certify your switch. Administrators will be warned that the certificate has not been certified by a Certificate Authority (CA), but security will not be otherwise affected.

If you cannot generate an X.509 certificate yourself, you can buy one from one of the Certifying Authorities or your ISP. Each switch requires its own X.509 certificate.

To download an HTTPS certificate:

1 Click **Security > HTTPS Settings > Download Certificate**. The *HTTPS Download Certificate Page* opens:

Figure 39 HTTPS Download Certificate Page



This downloads a new HTTPS server certificate from the file specified.

Note: The unit will have to reboot before the new certificate can be used.

TFTP Server Details:

IP Address	0.0.0.0
Certificate Filename	
Private Key Filename	
Private Key Password	

The *HTTPS Download Certificate Page* contains the following fields:

- IP Address — Network address of a TFTP server.
- Certificate Filename — Filename of the digital certificate.
- Private Key Filename — Name of file containing the certificate.

- Private Key Password — Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.

2 Define the fields.

3 Click Apply. The certificate is downloaded.

You must reboot the switch to start using the new certificate.

Using the Secure Shell Protocol (SSH)

Secure Shell (SSH) provides a secure replacement for management access via Telnet. When an SSH management client contacts the switch, the switch first compares the public-key and password provided by the client against those stored locally before granting access. SSH also encrypts all data transfers passing between the switch and SSH management clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

The switch supports both SSH Version 1.5 and 2.0 clients.

The SSH server on this switch supports local password authentication. Note that although the switch only supports password authentication, you still have to generate a public key on the switch.

To use the SSH server, complete these steps:

1 Generate a Host Key Pair – No keys are generated in the switch's factory default configuration. You must use the *SSH Key Generate Page* to create a public host key.

2 Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35
15684995401867669259333946775054617325313674890836547254150202455
93199868544358361651999923329781766065830956108259132128902337654
68017262725714134287629413011961955667825956641048695742788814620
65194174677298486546861571773939016477935594230357741309802273708
779454524083971752646358058176716709574804776117
```

Password Authentication (for SSH v1.5 or V2 Clients)

a The client sends its password to the server.

b The switch compares the client's password to those stored in memory.

c If a match is found, the connection is allowed.

To use SSH with password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. You do not need to configure the client's keys.

The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

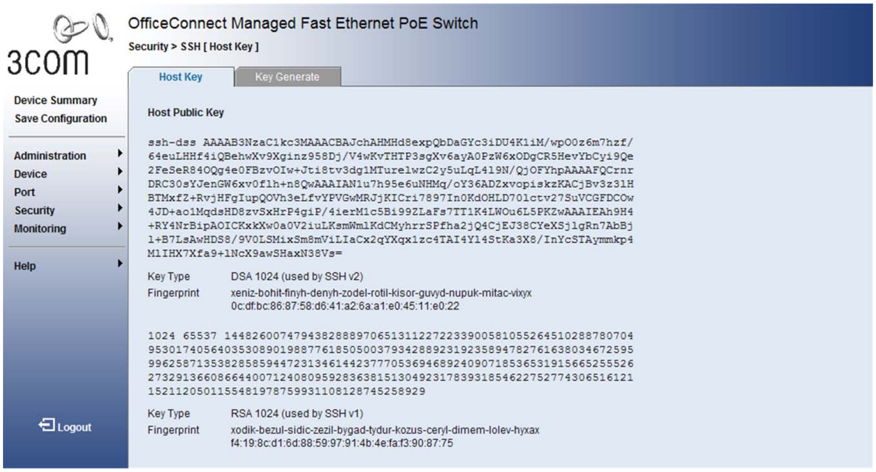
Displaying the SSH Key

The *SSH Host Key Page* shows the public key used for management access to the switch through an SSH client application.

To view the DSA and RSA keys:

1 Click **Security > SSH > Host Key**. The *SSH Host Key Page* opens:

Figure 40 SSH Host Key Page



Host Public Key

```
ssh-dss AAAAB3NzaC1kc3MAAACBAJchAHMHd8expQbDaGYc3iDU4K1iM/wpO0z6m7hzf/
64euLHHf4iQBehwXv9Xginz958Dj/V4wKvTHTP3sgXv6ayA0PzW6xODgCR5HevYbCyi9Qe
2FeSeR84OQg4e0FBzvOIw+Jti8tv3dg1MTurelwzC2y5uLqL419N/QjOFYhpAAAAFQCrnr
DRC30sYJenGW6xv0f1h+n8QwAAAIAN1u7h95e6uNHMq/oY36ADZxvopiskzKACjBv3z31H
BTMxfZ+RvjHFgIupQOVh3eLfvYPVGwMRJjKICri7897In0KdOHLD701ctv27SuVCGFDCOw
4JD+ao1MqdsHD8zvSxHrP4giP/4ierM1c5Bi99ZLaFs7TT1K4LWOu6L5PKZwAAAIEAh9H4
+RY4NrBipAOICKxkXw0a0V2iuLKsmWmlKdCMyhrrSPfha2jQ4CjEJ38CYeXSj1gRn7AbBj
1+B7LsAwHDS8/9V0LSMixSm8mViLIaCx2qYXqx1zc4TAI4Y14StKa3X8/InYcSTAymmkp4
M1IHX7Xfa9+1NcX9awSHaxN38Vs=
```

Key Type DSA 1024 (used by SSH v2)

Fingerprint xeniz-bohit-finyh-denyh-zodel-rotil-kisor-guvyd-nupuk-mitac-vixyx
0c:df:bc:86:87:58:d6:41:a2:6a:a1:e0:45:11:e0:22

```
1024 65537 14482600747943828889706513112272233900581055264510288780704
9530174056403530890198877618505003793428892319235894782761638034672595
9962587135382858594472313461442377705369468924090718536531915665255526
2732913660866440071240809592836381513049231783931854622752774306516121
1521120501155481978759931108128745258929
```

Key Type RSA 1024 (used by SSH v1)

Fingerprint xodik-bezul-sidic-zezil-bygad-tydur-kozus-ceryl-dimem-lolev-hyxax
f4:19:8c:d1:6d:88:59:97:91:4b:4e:fa:f3:90:87:75

The *SSH Host Key Page* contains the following fields:

- **Key** — When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.
- **Key Type** — Indicates DSA or RSA key type, the key size, and the SSH client versions which may use this key.
- **Fingerprint** — Hash algorithms used to generate the key.

Generating the SSH Key

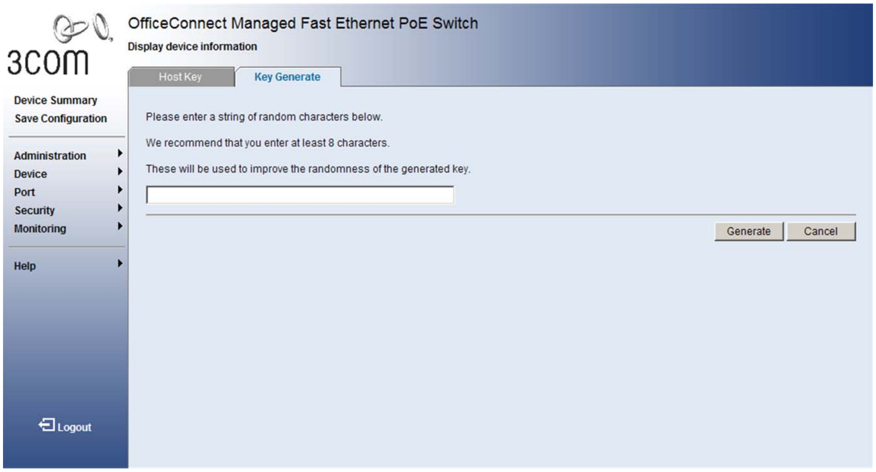
The *SSH Key Generate Page* generates both the DSA and RSA key pairs. No keys are generated in the switch's factory default configuration. You must use this web page to create a public host key.

Gererating a SSH key can take up to 15 minutes, during which time the user interface to the switch may not respond.

To generate DSA and RSA keys:

1 Click **Security > SSH >** Generate. The *SSH Key Generate Page* opens:

Figure 41 SSH Key Generate Page



Please enter a string of random characters below.

We recommend that you enter at least 8 characters.

These will be used to improve the randomness of the generated key.

The *SSH Key Generate Page* contains a prompt message to enter a seed to randomize the key generation process:

2 Enter any random string, preferably eight characters or more.

3 Click Generate. The switch begins generating the public host key. This process takes several minutes to complete. After the key is generated, it is stored in flash memory.

The SSH server on the switch uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.

Defining Access Control Lists

Access Control Lists (ACLs) allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port, with an active ACL are either admitted or denied entry.

For example, an ACL rule states that port number 20 can receive TCP packets, however, if a UDP packet is received, the packet will be dropped. ACLs are composed of access control entries (ACEs) that are made of the filters that determine traffic classifications.

The following are examples of filters that can be defined as ACEs:

- **Source Port IP Address and Wildcard Mask** — Filters packets by the source port IP address and wildcard mask.
- **Destination Port IP Address and Wildcard Mask** — Filters packets by the destination port IP address and wildcard mask.
- **Protocol** — Filters packets by the IP protocol.
- **DSCP** — Filters packets by the DiffServ Code Point (DSCP) value.
- **IP Precedence** — Filters packets by the IP Precedence.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped.

This section includes the following topics:

- Viewing MAC Based ACLs
- Configuring MAC Based ACLs
- Removing MAC Based ACLs
- Viewing IP Based ACLs
- Defining IP Based ACLs
- Removing IP Based ACLs
- Viewing ACL Binding
- Configuring ACL Binding
- Removing ACL Binding

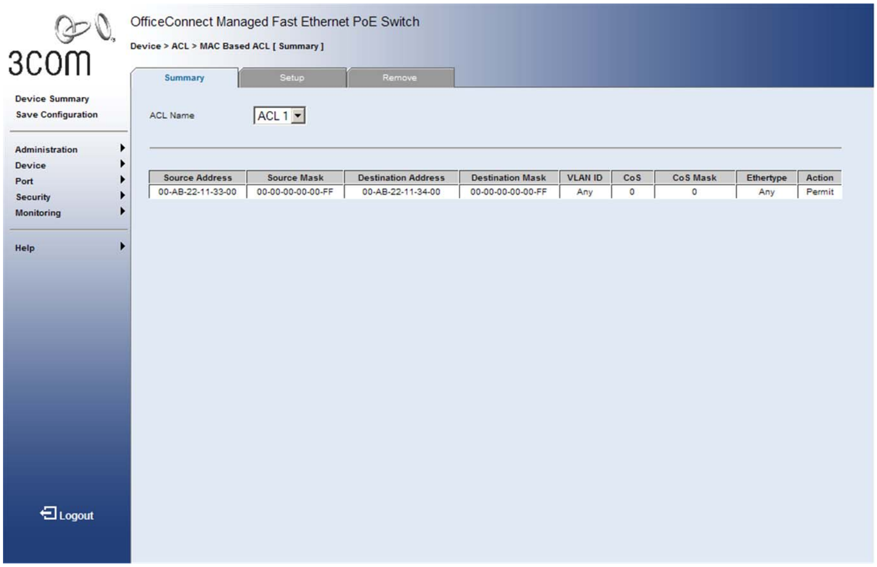
Viewing MAC Based ACLs

The *MAC Based ACL Summary Page* displays information regarding MAC Based ACLs configured on the device.

To view MAC Based ACLs:

1 Click **Device > ACL > MAC Based ACL > Summary**. The *MAC Based ACL Summary Page* opens:

Figure 42 MAC Based ACL Summary Page



ACL Name: ACL 1

Source Address	Source Mask	Destination Address	Destination Mask	VLAN ID	CoS	CoS Mask	Ethertype	Action
00-AB-22-11-33-00	00-00-00-00-00-FF	00-AB-22-11-34-00	00-00-00-00-00-FF	Any	0	0	Any	Permit

The *MAC Based ACL Summary Page* contains the following fields:

- **ACL Name** — Contains a list of the MAC-based ACLs.
- **Source Address** — Indicates the source MAC address.
- **Source Mask** — Indicates the source MAC address Mask.
- **Destination Address** — Indicates the destination MAC address.
- **Destination Mask** — Indicates the destination MAC address Mask.
- **VLAN ID** — Matches the packet's VLAN ID to the ACL rule. The possible field values are *0* to *4095*.
- **CoS** — Classifies traffic based on the CoS tag value.
- **CoS Mask** — Displays the CoS mask used to filter CoS tags.
- **Ethertype** — Provides an identifier that differentiates between various types of protocols.

- **Action** — Indicates the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

Configuring MAC Based ACLs

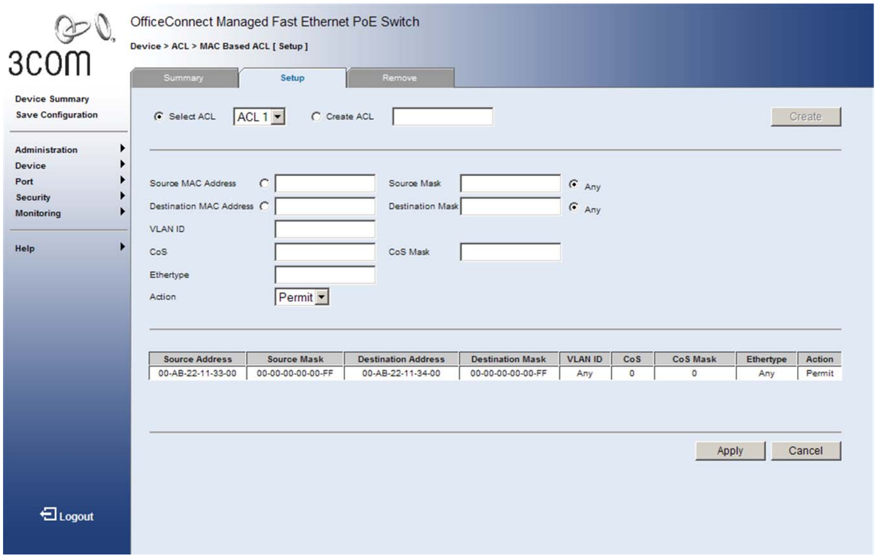
The *MAC Based ACL Setup Page* allows the network administrator to create and define rules for MAC-based ACLs.

Monitor users have no access to this page.

To configure MAC-based ACLs:

Click **Device > ACL > MAC Based ACL > Setup**. The *MAC Based ACL Setup Page* opens:

Figure 43 MAC Based ACL Setup Page



● Select ACL ACL 1 ○ Create ACL

Source MAC Address ○ Source Mask ● Any

Destination MAC Address ○ Destination Mask ● Any

VLAN ID

CoS CoS Mask

Ethertype

Action Permit

Source Address	Source Mask	Destination Address	Destination Mask	VLAN ID	CoS	CoS Mask	Ethertype	Action
00-AB-22-11-33-00	00-00-00-00-00-FF	00-AB-22-11-34-00	00-00-00-00-00-FF	Any	0	0	Any	Permit

The *MAC Based ACL Setup Page* contains the following fields:

- **Select ACL** — Selects an existing MAC-based ACL to which rules are to be added.
- **Create ACL** — Defines a new user-defined MAC-based ACL.

Add Rules to ACL

- **Source MAC Address** — Matches the source MAC address to which packets are addressed.
- **Source Mask** — Defines the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source MAC address. Wildcard masks specify which bits are used and which are ignored. A wildcard mask of FF:FF:FF:FF:FF:FF indicates that all the bits are important. A wildcard of 00.00.00.00.00.00.00 indicates that no bits are important. For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is FF:FF:FF:FF:FF:00, the first five bytes of the MAC are used, while the last byte is ignored. For the source MAC address 00:AB:22:11:33:00, this wildcard mask matches all MAC addresses in the range 00:AB:22:11:33:00 to 00:AB:22:11:33:FF.
- **Destination MAC Address** — Matches the destination MAC address to which packets are addressed.
- **Destination Mask** — Defines the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination MAC address. Wildcard masks specify which bits are used and which are ignored. For more details, refer to the description for Source Mask.
- **VLAN ID** — Matches the packet's VLAN ID. The possible field values are 0 to 4095.
- **CoS** — Classifies traffic based on the CoS tag value. The possible field values are 0 to 7.
- **CoS Mask** — Defines the CoS mask used to classify network traffic. The possible field values are 0 to 7.
- **Ethertype** — Provides an identifier that differentiates between various types of protocols. The range is *0-65535* decimal.
- **Action** — Specifies the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

To create a new MAC-based ACL:

1. Select *Create ACL*.
2. Enter the name of the new ACL.
3. Click Create. The new ACL is created, and the device is updated.

To define a new MAC-based ACL rule:

1 Select *Select ACL*.

2 Select the ACL from the list.

3 Define the fields for the new ACL rule.

4 Click Apply. The new MAC-based ACL rule settings are configured, and the device is updated.

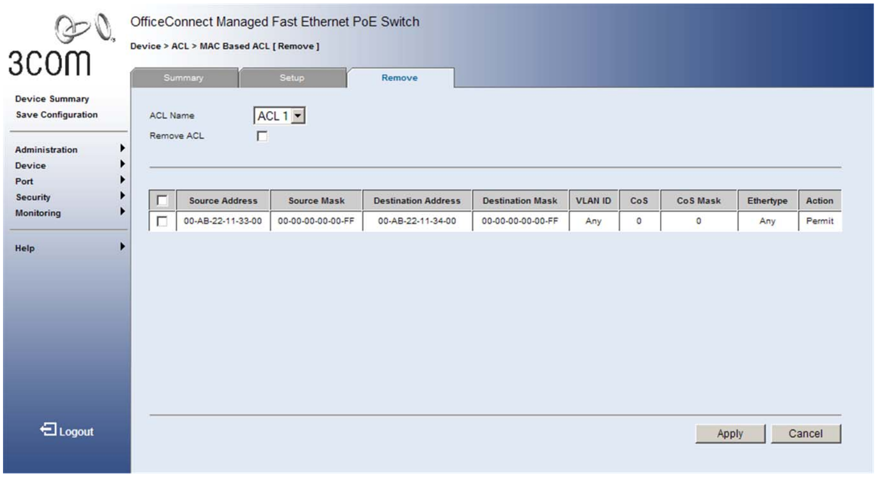
Removing MAC Based ACLs

The MAC Based ACL Remove Page allows the network administrator to remove MAC-based ACLs or MAC-based ACL rules.

Monitor users have no access to this page.

Click **Device > ACL > MAC Based ACL > Remove**. The *MAC Based ACL Remove Page* opens:

Figure 44 MAC Based ACL Remove Page



ACL Name: ACL 1
Remove ACL: □

□	Source Address	Source Mask	Destination Address	Destination Mask	VLAN ID	CoS	CoS Mask	Ethertype	Action
□	00-AB-22-11-33-00	00-00-00-00-00-FF	00-AB-22-11-34-00	00-00-00-00-00-FF	Any	0	0	Any	Permit

The MAC Based ACL Remove Page contains the following fields:

- **ACL Name** — Selects a MAC-based ACL for removal.
- **Remove ACL** — Enables the ACL to be removed.
- Checkbox (unnamed) — When checked, selects the rule for removal. The top checkbox is used to select all rules for removal.
- **Source Address** — Matches the source MAC address to which packets are addressed.
- **Source Mask** — Matches the source MAC address Mask.

- **Destination Address** — Matches the destination MAC address to which packets are addressed.
- **Destination Mask** — Matches the destination MAC address Mask.
- **VLAN ID** — Matches the packet's VLAN ID to the rule.
- **CoS** — Classifies Class of Service of the packet.
- **CoS Mask** — Displays the wildcard mask bits to be applied to the CoS.
- **Ethertype** — Provides an identifier that differentiates between various types of protocols.
- **Action** — Indicates the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

To remove MAC-based ACLs:

1. Select the *ACL Name* to be deleted.
2. Check *Remove ACL*.
3. Click Remove. The selected ACL is deleted, and the device is updated.

To remove MAC-based ACL rules:

1. Select the *ACL Name* containing the rules to be deleted.
2. For each rule to be removed, check the box to the left of the row in the rules table. To remove all rules, the topmost box may be checked.
3. Click Remove. The selected MAC-based ACL rules are deleted, and the device is updated.

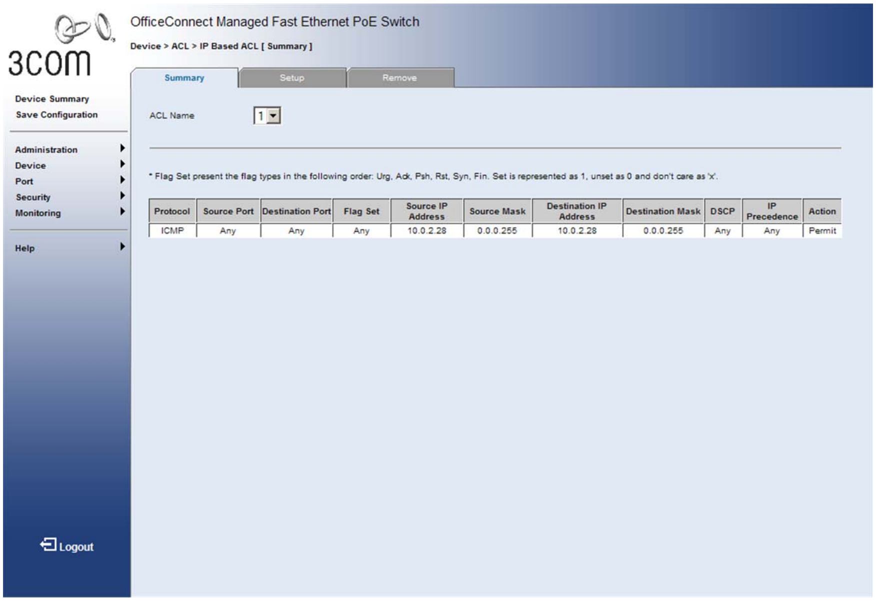
Viewing IP Based ACLs

The *IP Based ACL Summary Page* displays information regarding IP-based ACLs configured on the device.

To view IP-based ACLs:

1 Click **Device > ACL > IP Based ACL > Summary**. The *IP Based ACL Summary Page* opens:

Figure 45 IP Based ACL Summary Page



ACL Name 1

* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

Protocol	Source Port	Destination Port	Flag Set	Source IP Address	Source Mask	Destination IP Address	Destination Mask	DSCP	IP Precedence	Action
ICMP	Any	Any	Any	10.0.2.28	0.0.0.255	10.0.2.28	0.0.0.255	Any	Any	Permit

The *IP Based ACL Summary Page* contains the following fields:

- **ACL Name** — Contains a list of the IP Based ACLs.
- **Protocol** — Indicates the protocol in the rule to which the packet is matched.
- **Source Port** — Indicates the source port to match in packets. Enabled only when TCP or UDP are selected in the Protocol list.
- **Destination Port** — Indicates the destination port to match in packets. Enabled only when TCP or UDP are selected in the Protocol list.
- **Flag Set** — Indicates the TCP flag to which the packet is mapped.
- **Source IP Address** — Matches the source IP address to which packets are addressed.
- **Source Mask** — Indicates the source IP address mask.

- **Dest. IP Address** — Matches the destination IP address to which packets are addressed.
- **Destination Mask** — Indicates the destination IP address mask.
- **Match DSCP** — Matches the packet DSCP value.
- **Match IP Precedence** — Indicates matching IP Precedence with the packet IP precedence value.
- **Action** — Indicates the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

Defining IP Based ACLs

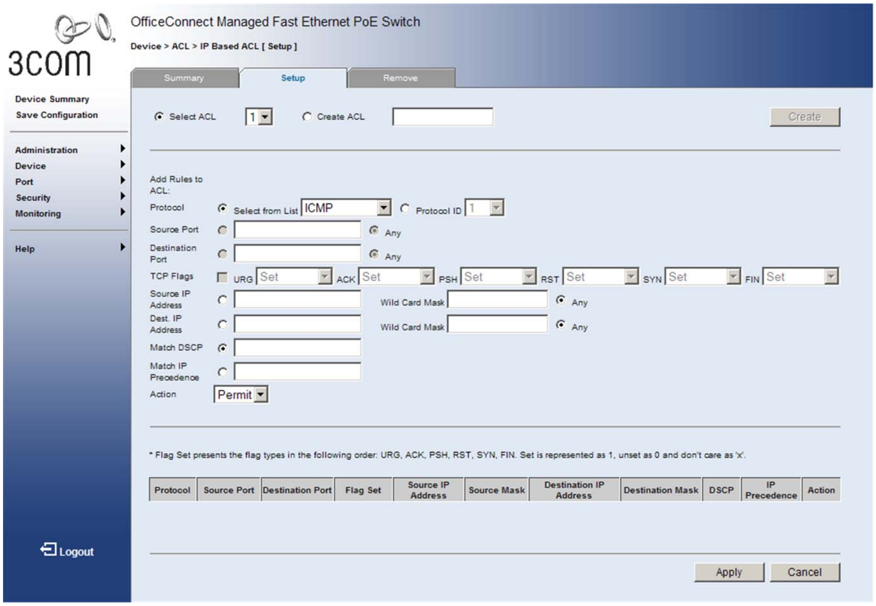
Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 256 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. ACLs are composed of access control entries (ACEs) that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 256.

Monitor users have no access to this page.

To configure IP-based ACLs:

Click **Device > ACL > IP Based ACL > Setup**. The *IP Based ACL Setup Page* opens:

Figure 46 IP Based ACL Setup Page



● Select ACL [1] ○ Create ACL [ ]

Add Rules to ACL:

Protocol ● Select from List [ICMP] ○ Protocol ID [1]

Source Port ○ [ ] ● Any

Destination Port ○ [ ] ● Any

TCP Flags □ URG [Set] ACK [Set] PSH [Set] RST [Set] SYN [Set] FIN [Set]

Source IP Address ○ [ ] Wild Card Mask [ ] ● Any

Dest. IP Address ○ [ ] Wild Card Mask [ ] ● Any

Match DSCP ● [ ]

Match IP Precedence ○ [ ]

Action [Permit]

* Flag Set presents the flag types in the following order: URG, ACK, PSH, RST, SYN, FIN. Set is represented as 1, unset as 0 and don't care as 'x'.

Protocol	Source Port	Destination Port	Flag Set	Source IP Address	Source Mask	Destination IP Address	Destination Mask	DSCP	IP Precedence	Action

The *IP Based ACL Setup Page* contains the following fields:

- **Select ACL** — Selects an existing IP-based ACL to which rules are to be added.
- **Create ACL** — Defines a new user-defined IP-based ACL.

Add Rules to ACL

- **Protocol** — Defines the protocol in the rule to which the packet is matched. The possible fields are:
  - *Select from List* — Selects a protocol from a list by which packets are matched.
  - *Protocol ID* — Adds user-defined protocols by which packets are matched. Each protocol has a specific protocol number which is unique. The possible field range is *0-255*.
- **Source Port** — Defines the source port that is used for matched packets. Enabled only when TCP or UDP are selected in the Protocol list. The field value is either user defined or *Any*. If *Any* is selected the IP based ACL is applied to any source port.
- **Destination Port** — Defines the destination port that is used for matched packets. Enabled only when TCP or UDP are selected in the Protocol list. The field value is either user defined or *Any*. If *Any* is selected, the IP based ACL is applied to any destination port.
- **TCP Flags** — If checked, enables configuration of TCP flags matched to the packet. The possible fields are:
  - *URG* — Urgent pointer field significant. The urgent pointer points to the sequence number of the octet following the urgent data.
  - *ACK* — Acknowledgement field significant. The acknowledgement field is the byte number of the next byte that the sender expects to receive from the receiver.
  - *PSH* — Push (send) the data as soon as possible, without buffering. This is used for interactive traffic.
  - *RST* — Reset the connection. This invalidates the sequence numbers and aborts the session between the sender and receiver.
  - *SYN* — Synchronize Initial Sequence Numbers (ISNs). This is used to initialize a new connection.
  - *FIN* — Finish. This indicates there is no more data from the sender. This marks a normal closing of the session between the sender and receiver.

  For each TCP flag, the possible field values are:

  - *Set* — Enables the TCP flag.
  - *Unset* — Disables the TCP flag.
  - *Don’t Care* — Does not check the packet’s TCP flag.

- **Source IP Address** — If selected, enables matching the source port IP address to which packets are addressed to the rule, according to a wildcard mask. The field value is either user defined or *Any*. If *Any* is selected, accepts any source IP address and disables wildcard mask filtering.
  - *Wild Card Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that all the bits are important. A wildcard mask of 0.0.0.0 indicates that no bits are important. For example, if the source IP address is 149.36.184.198 and the wildcard mask is 255.255.255.0, the first three bytes of the IP address are matched, while the last eight bits are ignored. For the source IP address 149.36.184.198, this wildcard mask matches all IP addresses in the range 149.36.184.0 to 149.36.184.255. A wildcard mask must not contain leading zeroes. For example, a wildcard mask of 010.010.011.010 is invalid, but a wildcard mask of 10.10.11.10 is valid.
- **Destination IP Address** — If selected, enables matching the destination port IP address to which packets are addressed to the rule, according to a wildcard mask. The field value is either user defined or *Any*. If *Any* is selected, accepts any destination IP address and disables wildcard mask filtering.
  - *Wild Card Mask* — Indicates the destination IP Address wildcard mask. Wildcards are used to mask all or part of a destination IP Address. Wildcard masks specify which bits are used and which bits are ignored. For more details, refer to the description for wildcard masks under Source IP Address.
- **Match DSCP** — Matches the packet DSCP value to the ACL. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is *0-7*.
- **Match IP Precedence** — Matches the packet IP Precedence value to the rule. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is *0-63*.
- **Action** — Defines the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

To create a new IP-based ACL:

1 Select *Create ACL*.

2 Enter the name of the new ACL.

3 Click Create. The new ACL is created, and the device is updated.

To define a new IP-based ACL rule:

1 Select *Select ACL*.

2 Select the ACL from the list.

3 Define the fields for the new ACL rule.

4 Click Apply. The new IP-based ACL rule settings are configured, and the device is updated.

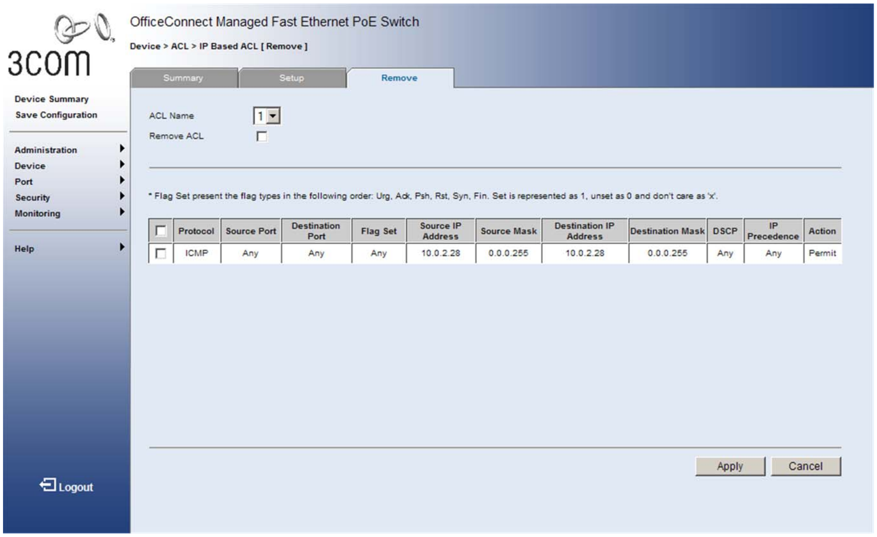
Removing IP Based ACLs

The *IP Based ACL Remove Page* allows the user to remove IP-based ACLs or IP-based ACL rules.

Monitor users have no access to this page.

Click **Device > ACL > IP Based ACL > Remove**. The *IP Based ACL Remove Page* opens:

Figure 47 IP Based ACL Remove Page



ACL Name 1

Remove ACL □

* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

□	Protocol	Source Port	Destination Port	Flag Set	Source IP Address	Source Mask	Destination IP Address	Destination Mask	DSCP	IP Precedence	Action
□	ICMP	Any	Any	Any	10.0.2.28	0.0.0.255	10.0.2.28	0.0.0.255	Any	Any	Permit

The *IP Based ACL Remove Page* contains the following fields:

- **ACL Name** — Selects an ACL name from a list of the IP-based ACLs.
- **Remove ACL** — Enables the ACL to be removed.
- Checkbox (unnamed) — When checked, selects the rule for removal. The top checkbox is used to select all rules for removal.
- **Protocol** — Indicates the protocol in the rule to which the packet is matched.
- **Source Port** — Displays the TCP/UDP source port to which the ACL is matched.
- **Destination Port** — Displays the TCP/UDP destination port.
- **Flag Set** — Indicates the TCP flag matched to the packet.
- **Source IP Address** — Indicates the source IP address.
- **Source Mask** — Indicates the source IP address mask.
- **Destination IP Address** — Indicates the destination IP address.
- **Destination Mask** — Indicates the destination IP address mask.
- **DSCP** — Matches the packet DSCP value to the ACL. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.
- **IP Precedence** — Matches the packet IP Precedence value to the ACL.
- **Action** — Indicates the ACL forwarding action. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.

To remove an IP-based ACL:

1. Select an ACL Name to be removed.
2. Check *Remove ACL*.
3. Click Remove. The selected ACL is deleted, and the device is updated.

To remove IP-based ACL rules:

1. Select an ACL Name.
2. For each rule to be removed, check the box to the left of the row in the rules table. To remove all rules, the topmost box may be checked.
3. Click Remove. The selected ACL rules are deleted, and the device is updated.

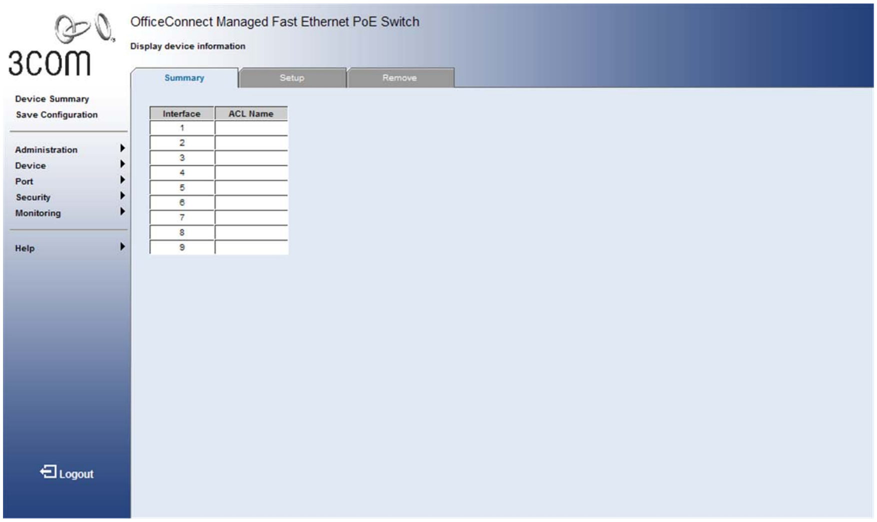
Viewing ACL Binding

The *ACL Binding Summary Page* displays the user-defined ACLs mapped to the interfaces.

To view ACL Binding:

1 Click **Device > ACL > ACL Binding > Summary**. The *ACL Binding Summary Page* opens:

Figure 48 ACL Binding Summary Page



Interface	ACL Name
1	
2	
3	
4	
5	
6	
7	
8	
9	

The *ACL Binding Summary Page* contains the following fields:

- **Interface** — Displays the port or LAG number to which the ACL is bound.
- **ACL Name** — Displays the name of the ACL which is bound to a selected port or LAG.

Configuring ACL Binding

After configuring the required ACLs, you should bind them to the ports or LAGs that need to filter traffic. You can only bind an interface to one ACL for each basic type – IP and MAC.

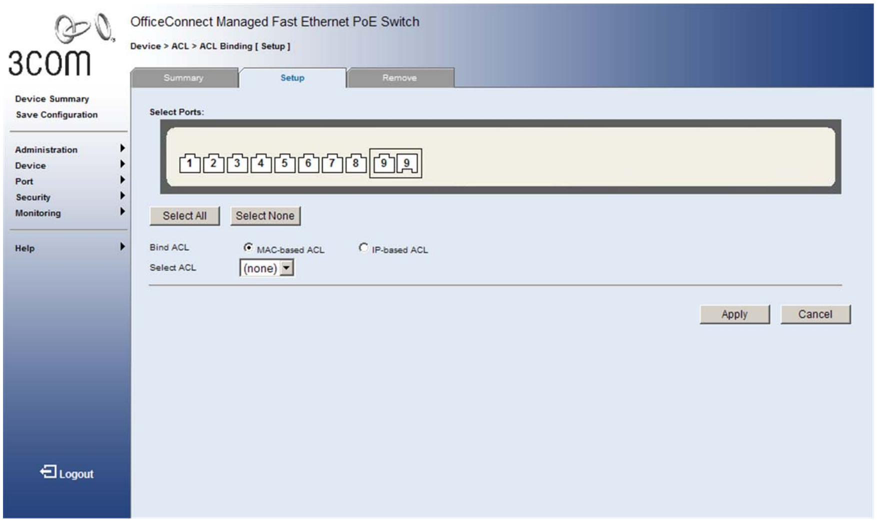
The *ACL Binding Setup Page* allows the network administrator to bind specific ports to MAC- or IP-based ACLs.

Monitor users have no access to this page.

To define ACL Binding:

1 Click **Device > ACL > ACL Binding > Setup**. The *ACL Binding Setup Page* opens:

Figure 49 ACL Binding Setup Page



Bind ACL ● MAC-based ACL ○ IP-based ACL
Select ACL (none)

The *ACL Binding Setup Page* contains the following fields:

- **Select Port(s)** — Selects the ports to be configured.
- **Bind ACL** — Assigns an Access Control List to a port or LAG.
  - *MAC-based ACL* — Displays the MAC based ACL to which the interface is assigned.
  - *IP-based ACL* — Displays the IP based ACL to which the interface is assigned.
- **Select ACL** — Selects the ACL from a list of previously defined Access Control Lists to which the port or LAG can be bound. To bind an ACL to a LAG, the ACL should be bound to its port members.

2 Define the relevant fields.

3 Click Apply. ACL Binding is defined, and the device is updated.

Removing ACL Binding

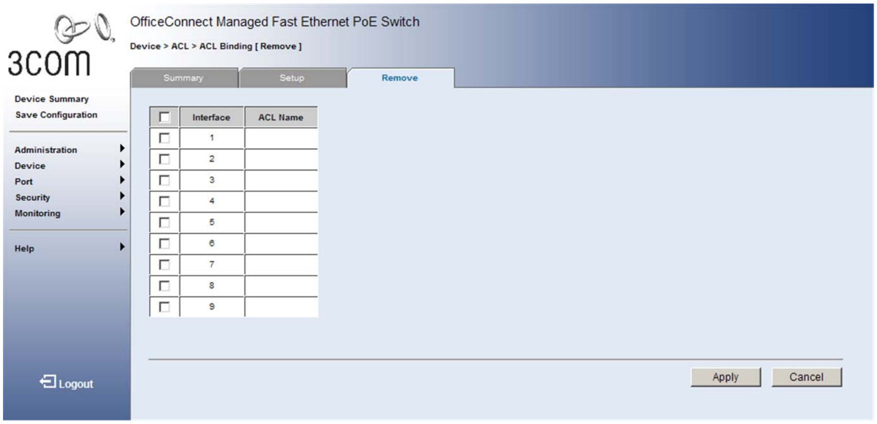
The *ACL Binding Remove Page* allows the network administrator to remove user-defined ACLs from a selected interface.

Monitor users have no access to this page.

To remove ACL Binding:

1 Click **Device > ACL > ACL Binding > Remove**. The *ACL Binding Remove Page* opens:

Figure 50 ACL Binding Remove Page



□	Interface	ACL Name
□	1	
□	2	
□	3	
□	4	
□	5	
□	6	
□	7	
□	8	
□	9	

The *ACL Binding Remove Page* contains the following fields:

- Checkbox (unnamed) — Marks the ACL for removal.
- **Interface** — Displays the port interface to which the ACL is bound.
- **ACL Name** — Displays the name of ACL to be removed from the selected port.

2 For each ACL to be removed, check the box to the left of the row in the table. To remove all ACLs, the topmost box may be checked.

3 Click Remove. The selected ACLs are removed, and the device is updated.

Using Broadcast Storm Control

Broadcast Storm Control limits the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Broadcast Storm Control is enabled for all ports by defining the packet type and the maximum rate at which the packets can be transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

The packet threshold is ignored if Broadcast Storm Control is Disabled.

Displaying Broadcast Storm Control Settings

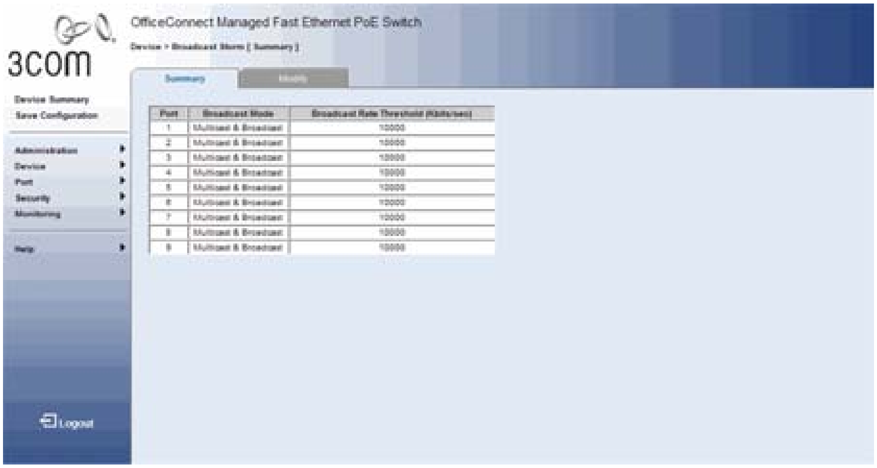
The *Broadcast Storm Summary Page* displays the storm control settings for all ports.

Monitor users have no access to this page.

To display the storm control settings:

1. Click **Device > Broadcast Storm > Summary**. The *Broadcast Storm Summary Page* opens:

Figure 51 Broadcast Storm Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > Broadcast Storm [Summary]

Port	Broadcast Mode	Broadcast Rate Threshold (Kbits/sec)
1	Multicast & Broadcast	10000
2	Multicast & Broadcast	10000
3	Multicast & Broadcast	10000
4	Multicast & Broadcast	10000
5	Multicast & Broadcast	10000
6	Multicast & Broadcast	10000
7	Multicast & Broadcast	10000
8	Multicast & Broadcast	10000
9	Multicast & Broadcast	10000

The *Broadcast Storm Summary Page* contains the following fields:

- **Port** — A list of interfaces.
- **Broadcast Mode** — The storm control mode used on a port.
- **Broadcast Rate Threshold** — The maximum rate (Kbits/sec) at which broadcast or multicast packets are forwarded.

Configuring Broadcast Storm Control

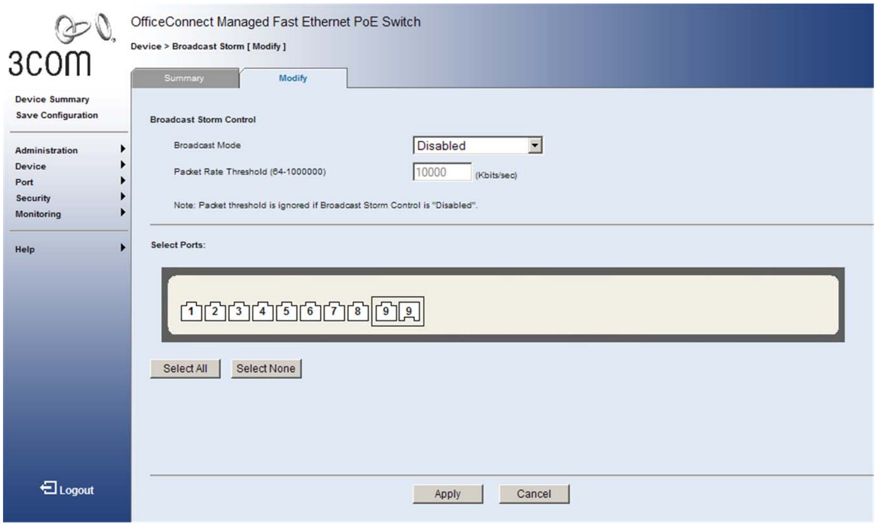
The *Broadcast Storm Modify Page* configures the storm control settings for all ports.

Monitor users have no access to this page.

To configure Broadcast Storm Control:

1 Click **Device > Broadcast Storm > Modify**. The *Broadcast Storm Modify Page* opens:

Figure 52 Broadcast Storm Modify Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > Broadcast Storm [Modify]

Broadcast Storm Control

Broadcast Mode: Disabled

Packet Rate Threshold (64-1000000): 10000 (Kbits/sec)

Note: Packet threshold is ignored if Broadcast Storm Control is "Disabled".

Select Ports:

The *Broadcast Storm Modify Page* contains the following fields:

- **Broadcast Mode** — Defines the storm control mode to use on the selected interface.
  - *Disabled* — Disables storm control on the selected port.
  - *Broadcast* — Enables broadcast storm control on the selected port.
  - *Broadcast&Multicast* — Enables broadcast and multicast storm control on the selected port.
- **Packet Rate Threshold** — Defines the maximum rate (kilobits per second) at which broadcast or multicast packets are forwarded. The range is *64-100,000* for Fast Ethernet ports, and *64-1,000,000* for Gigabit Ethernet ports. The default value is *10000*. Also note that the resolution at which this parameter can be configured is 64 kilobits.

2 Define the relevant fields.

3 Select the ports to which these settings will be applied.

4 Click Apply. Broadcast Storm Control is configured, and the device is updated.

5 MANAGING SYSTEM INFORMATION

This section contains information for configuring general system information, and includes the following:

- Viewing System Description
- Defining System Settings
- Saving the Device Configuration
- Resetting the Device

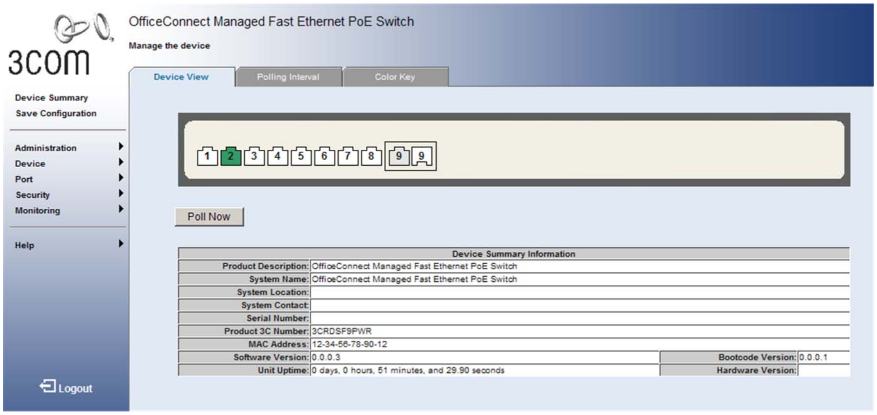
Viewing System Description

The *Device View Page* displays parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System Up Time, and MAC addresses, and both software, boot, and hardware versions.

To view Device Summary Information:

1 Click **Device Summary**. The *Device View Page* opens.

Figure 53 Device View Page



Device Summary Information			
Product Description:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Name:	OfficeConnect Managed Fast Ethernet PoE Switch		
System Location:			
System Contact:			
Serial Number:			
Product 3C Number:	3CRDSF9PWR		
MAC Address:	12-34-56-78-90-12		
Software Version:	0.0.0.3	Bootcode Version:	0.0.0.1
Unit Uptime:	0 days, 0 hours, 51 minutes, and 29.90 seconds	Hardware Version:	

The *Device View Page* contains the following fields:

- **Product Description** — Displays the device model number and name.
- **System Name** — Defines the user-defined device name. The field range is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.
- **Serial Number** — Displays the device serial number.
- **Product 3C Number** — Displays the 3Com device 3C number.
- **MAC Address** — Displays the device MAC address.
- **System Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.

- **Software Version** — Displays the installed software version number.
- **Boot Version** — Displays the current boot version running on the device.
- **Hardware Version** — Displays the current hardware version of the device.
- **Poll Now** — Enables polling the ports for port information including speed, utilization and port status.

Defining System Settings

The following section allows system administrators to configure advanced system settings. The section includes the following topics:

- Configuring the System Name
- Configuring System Time

Configuring the System Name

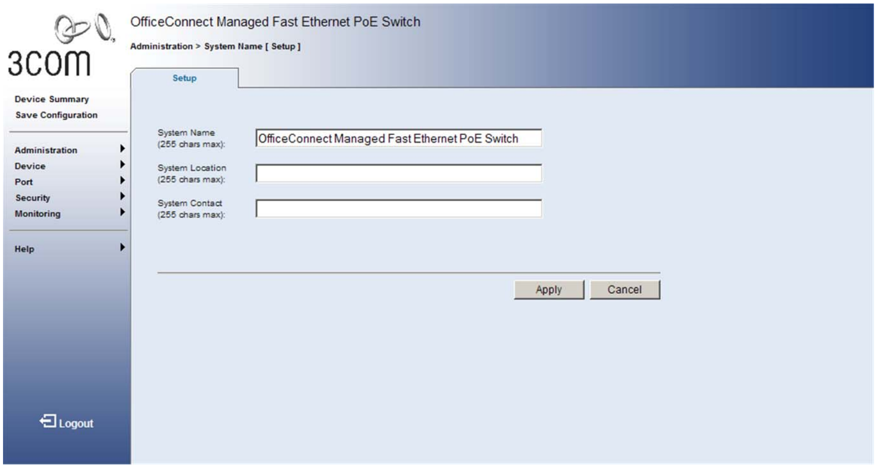
The *System Name Page* allows the Network Administrator to provide a user-defined system name, location, and contact information for the device.

Monitor users have no access to this page.

To configure the System Name:

1 Click **Administration > System Name > System Name**. The *System Name Page* opens:

Figure 54 System Name Page



System Name (255 chars max): OfficeConnect Managed Fast Ethernet PoE Switch

System Location (255 chars max):

System Contact (255 chars max):

The *System Name Page* includes the following fields:

- **System Name** — Defines the user-defined device name. The field length is 0-255 characters.
- **System Location** — Defines the location where the system is currently running. The field length is 0-255 characters.
- **System Contact** — Defines the name of the contact person. The field length is 0-255 characters.

2 Define the fields.

3 Click Apply. The System Name is enabled, and the device is updated.

Configuring System Time

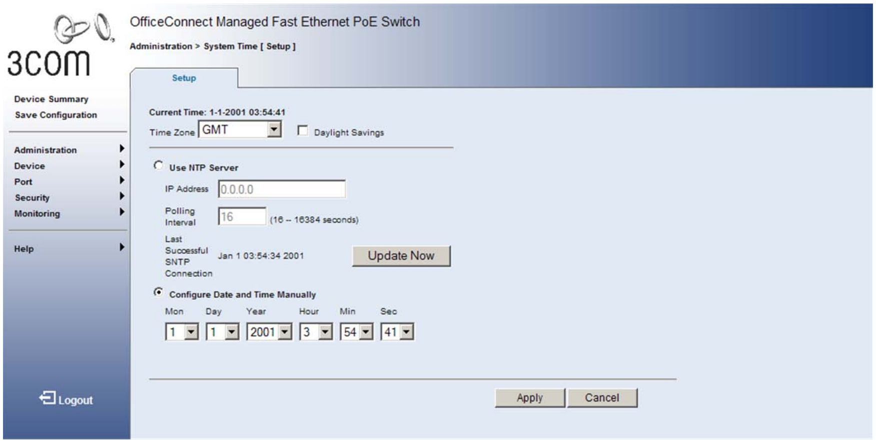
The *System Time Setup Page* contains fields that allow the network administrator to set the system clock by polling a time server or by manually configuring a specific time. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Monitor users have no access to this page.

To configure the System Time:

1 Click **Administration > System Time > Setup**. The *System Time Setup Page* opens:

Figure 55 System Time Setup Page



Current Time: 1-1-2001 03:54:41

Time Zone GMT ☐ Daylight Savings

○ Use NTP Server

IP Address 0.0.0.0

Polling Interval 16 (16 -- 16384 seconds)

Last Successful SNTP Connection Jan 1 03:54:34 2001

● Configure Date and Time Manually

Mon	Day	Year	Hour	Min	Sec
1	1	2001	3	54	41

The *System Time Setup Page* contains the following fields:

- **Current Time** — Displays the time set for the system clock.
- **Time Zone** — Name of time zone. The range for this field GMT -12 hours through GMT +13 hours, and the default is GMT.

  The local time zone is relative to Greenwich Mean Time, which is based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, indicate the number of hours your time zone is east (before) or west (after) of GMT.
- **Daylight Savings** — Specifies the use of daylight savings time to adjust the system clock

  In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Daylight Savings Time, or Summer Time. Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn. When enabled, the device switches to DST at 2:00 a.m. from the second Sunday in March, and reverts to standard time at 2:00 a.m. on the first Sunday of November.

- **Use NTP Server** — The system clock is set by dynamically polling a time server.
  - **IP Address** — IP address of an time server (NTP or SNTP). Note that up to three servers may be specified through the command line interface.
  - **Polling Interval** — Interval between time synchronization requests. The range for this field is *16-16384* seconds, and the default is *16* seconds.
  - **Last Successful SNTP Connection** — Displays the last time the switch's clock was successfully updated by a time server.
  - **Update Now** — Submits a time synchronization request to the configured time server.
- **Configure Date and Time Manually** — Manually sets the date and time used by the switch. This option may be used if there is no time server on your network, or if you need the switch to use a non-standard date or time.
  - **Month** — Sets the month. The field range is *1-12*.
  - **Day** — Sets the day. The field range is *1-31*.
  - **Year** — Sets the year. The field range is *2000-2037*.
  - **Hours** — Sets the hour. The field range is *0-23*.
  - **Min** — Sets the minutes. The field range is *0-59*.
  - **Sec** — Sets the seconds. The field range is *0-59*.

2 Define the fields.

3 Click Apply. The settings are saved, and the device is updated.

Saving the Device Configuration

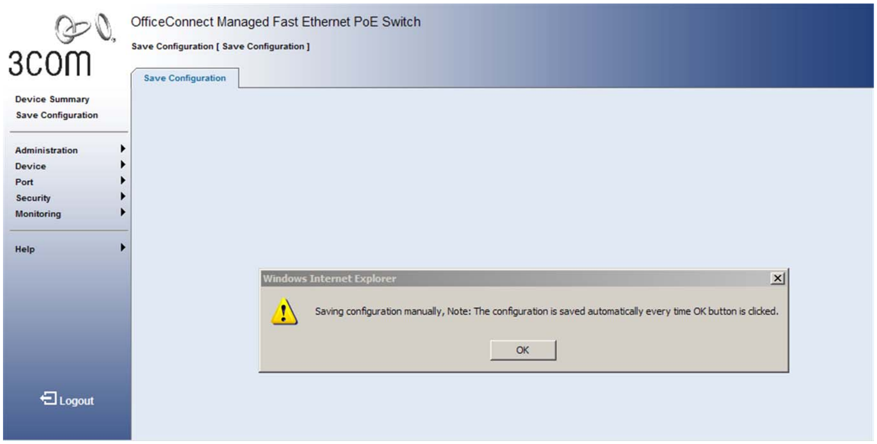
The *Save Configuration Page* allows the latest device configuration to be saved to the flash memory.

Monitor users have no access to this page.

To save the device configuration:

1 Click **Save Configuration**. The *Save Configuration Page* opens:

Figure 56 Save Configuration Page


3com
OfficeConnect Managed Fast Ethernet PoE Switch
Save Configuration [Save Configuration]
Save Configuration
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Windows Internet Explorer
OK

Saving configuration manually, Note: The configuration is saved automatically every time OK button is clicked.

The following message appears:

Saving configuration manually. Note: The configuration is saved automatically every time the OK button is clicked.

2 Click OK. The latest device configuration is saved, and the device is updated.

Resetting the Device

The *Reset Page* enables resetting the device from a remote location.

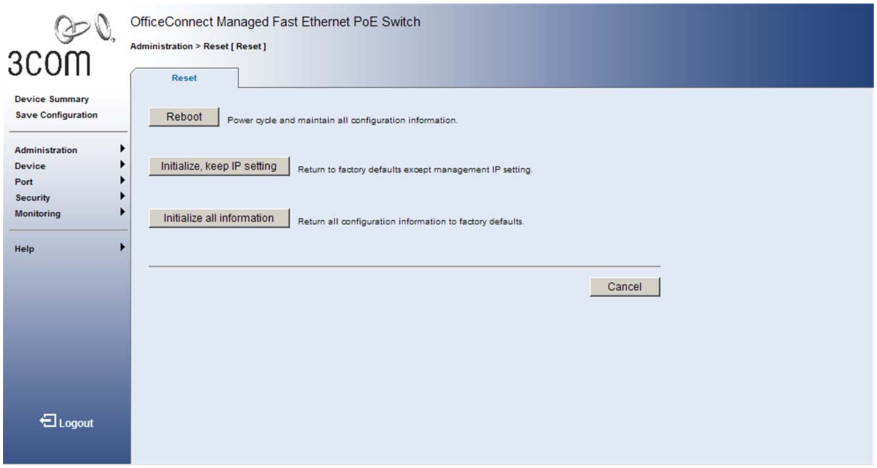
To prevent the current configuration from being lost, save the current device configuration before resetting the device.

Monitor users have no access to this page.

To reset the device configuration:

1 Click **Administration > Reset**. The *Reset Page* opens:

Figure 57 Reset Page



3com
OfficeConnect Managed Fast Ethernet PoE Switch
Administration > Reset [Reset]
Reset
Device Summary
Save Configuration
Administration
Device
Port
Security
Monitoring
Help
Logout
Reboot
Initialize, keep IP setting
Initialize all information
Cancel

Power cycle and maintain all configuration information.

Return to factory defaults except management IP setting.

Return all configuration information to factory defaults.

The *Reset Page* contains the following fields:

- **Reboot** — Reboots the device.
- **Initialize, keep IP Setting** — Resets the device with the factory default settings, but maintains the current IP Address.
- **Initialize all information** — Resets the device with the factory default settings, including the IP Address.

2 Click Reboot. The device is reset.

6 CONFIGURING PORTS

This section contains information for configuring Port Settings, and includes the following sections:

- Viewing Port Settings
- Defining Port Settings
- Viewing Port Details

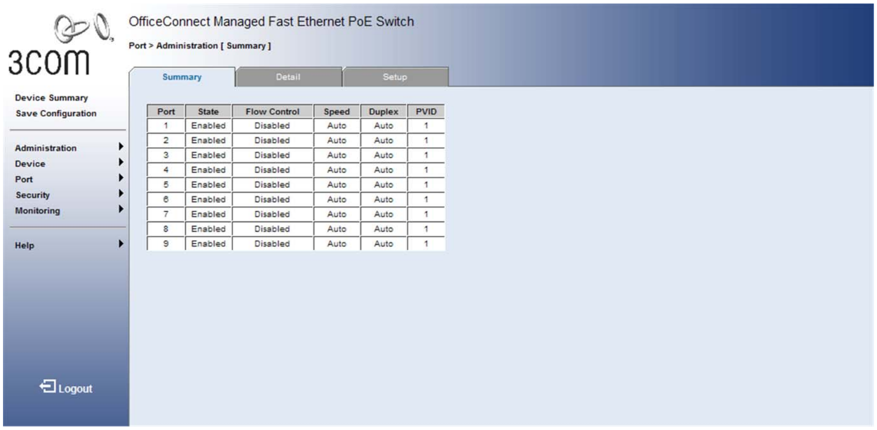
Viewing Port Settings

The *Port Administration Summary Page* permits the network manager to view current port configuration information.

To view Port Settings:

1 Click **Port > Administration > Summary**. The *Port Administration Summary Page* opens:

Figure 58 Port Administration Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Port > Administration [Summary]

Port	State	Flow Control	Speed	Duplex	PVID
1	Enabled	Disabled	Auto	Auto	1
2	Enabled	Disabled	Auto	Auto	1
3	Enabled	Disabled	Auto	Auto	1
4	Enabled	Disabled	Auto	Auto	1
5	Enabled	Disabled	Auto	Auto	1
6	Enabled	Disabled	Auto	Auto	1
7	Enabled	Disabled	Auto	Auto	1
8	Enabled	Disabled	Auto	Auto	1
9	Enabled	Disabled	Auto	Auto	1

The *Port Administration Summary Page* contains the following fields:

- **Port** — Indicates the selected port number.
- **State** — Shows if the interface is enabled or disabled.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode. The possible field values are:
  - *Enabled* — Enables flow control on the port.
  - *Disabled* — Disables flow control on the port.
- **Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. The possible field values are:
  - *10M* — Indicates the port is currently operating at 10 Mbps.
  - *100M* — Indicates the port is currently operating at 100 Mbps.
  - *1000M* — Indicates the port is currently operating at 1000 Mbps.
  - *Auto* — Indicates that port speed is set to an optimal value based on advertised capabilities.

- **Duplex** — Displays the port duplex mode. This field is configurable only when the port speed is set to 10M or 100M or 1000M per second. The possible field values are:
  - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
  - *Auto* — Indicates that port duplex mode is set to an optimal value based on advertised capabilities.
- **PVID** — VLAN ID assigned to untagged frames received on this port.

Defining Port Settings

The *Port Administration Setup Page* allows network managers to configure port parameters for specific ports.

Monitor users have no access to this page.

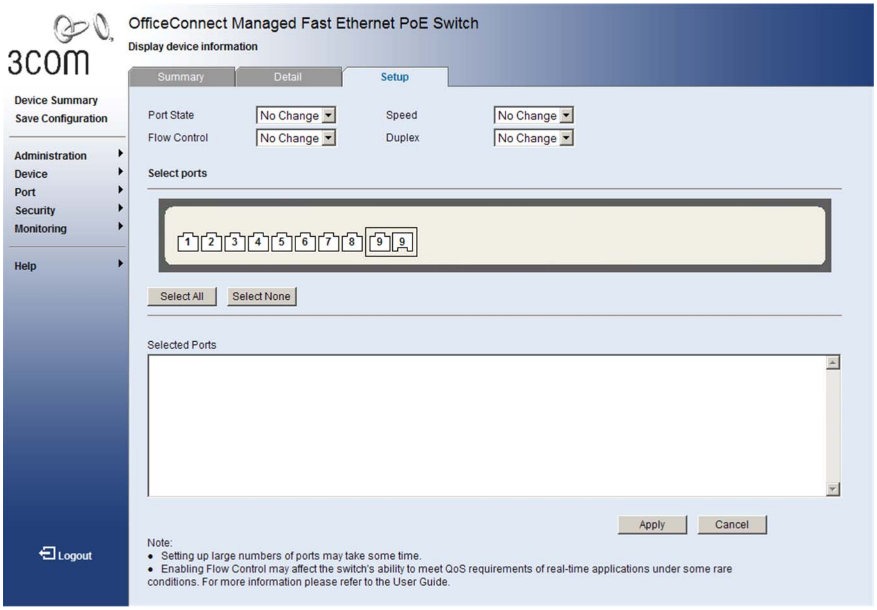
When using auto-negotiation to set the port speed or duplex mode, it must either be enabled for both parameters (Auto) or set to a fixed mode (10/100/1000, Half/Full).

The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed.

To configure Port Settings:

1 Click **Port > Administration > Setup**. The *Port Administration Setup Page* opens:

Figure 59 Port Administration Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Display device information

Port State: No Change

Flow Control: No Change

Speed: No Change

Duplex: No Change

Select ports

Selected Ports

Note:
- Setting up large numbers of ports may take some time.
- Enabling Flow Control may affect the switch's ability to meet QoS requirements of real-time applications under some rare conditions. For more information please refer to the User Guide.

The *Port Administration Setup Page* contains the following fields:

- **Port State** — Specifies the port state. The possible values are:
  - *Enabled* — Enables the port.
  - *Disabled* — Disables the port.
  - *No Change* — Retains the current port status.
- **Flow Control** — Specifies the flow control status on the port. Operates when the port is in full duplex mode. The possible field values are:
  - *Enabled* — Enables flow control on the port.
  - *Disabled* — Disables flow control on the port.
  - *No Change* — Retains the current flow control status on port.
- **Speed** — Specifies the configured rate for the port. The port type determines what speed setting options are available. The possible field values are:
  - *10* — Indicates the port is currently operating at 10 Mbps.
  - *100* — Indicates the port is currently operating at 100 Mbps.
  - *1000* — Indicates the port is currently operating at 1000 Mbps.
  - *Auto* — Use to automatically configure the port.
  - *No Change* — Retains the current port speed.
- **Duplex** — Specifies the port duplex mode. This field is configurable only when the port speed is set to 10M or 100M. The possible field values are:
  - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
  - *Auto* — Use to automatically configure the port.
  - *No Change* — Retains the current port duplex mode.
- **Select Ports** — Selects the ports to be configured.

2 Define the configuration fields.

3 Select the ports to which these settings will be applied.

4 Click Apply. The ports are configured, and the device is updated.

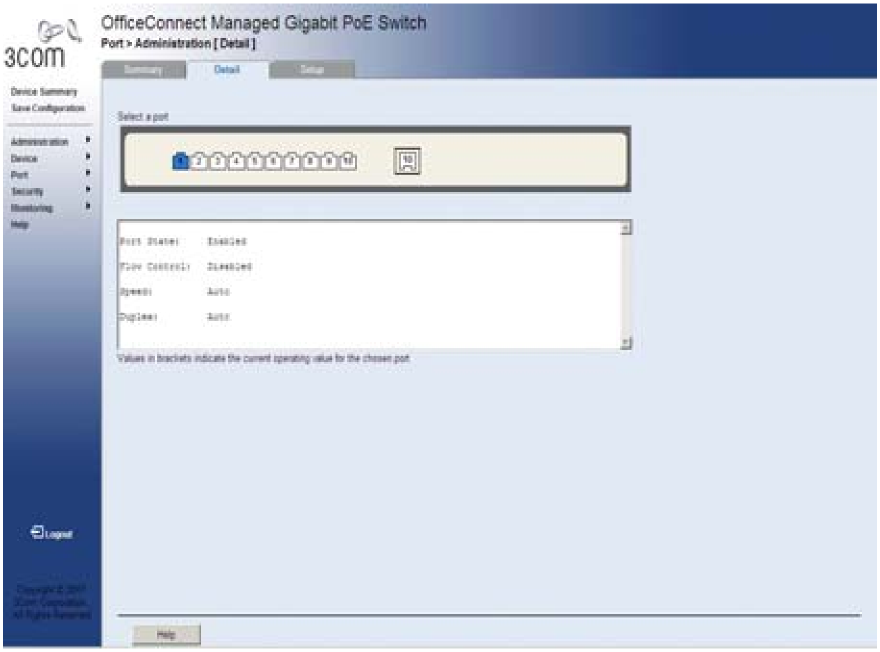
Viewing Port Details

The *Port Detail Page* displays the current port parameters for specific ports.

To view Port Details:

1 Click **Port > Administration > Detail**. The *Port Detail Page* opens:

Figure 60 Port Detail Page



OfficeConnect Managed Gigabit PoE Switch

Port > Administration [Detail]

Select a port

```
Port State:     Enabled
Flow Control:   Disabled
Speed:          Auto
Duplex:         Auto
```

Values in brackets indicate the current operating value for the chosen port

The *Port Detail Page* contains the following fields:

- **Select a port** — Selects a port to display its current settings.
- **Port State** — Indicates the port state. The possible field values are:
  - *Enabled* — Enables the port.
  - *Disabled* — Disables the port.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode. The possible field values are:
  - *Enabled* — Enables flow control on the port.
  - *Disabled* — Disables flow control on the port.

- **Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. The possible field values are:
  - *10* — Indicates the port is currently operating at 10 Mbps.
  - *100* — Indicates the port is currently operating at 100 Mbps.
  - *1000* — Indicates the port is currently operating at 1000 Mbps.
  - *Auto* — Used to automatically configure the port.
- **PVID** — VLAN ID assigned to untagged frames received on this port.
- **Link Type** — Displays the VLAN membership mode for a port. The possible field values are:
  - *Access* — The port transmits and receives untagged frames only.
  - *Hybrid* — The port may transmit tagged or untagged frames.
  - *Trunk* — The port is an end-point for a VLAN trunk. A VLAN trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN.
- **Duplex** — Displays the port duplex mode. This field is configurable only when the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
  - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
  - *Auto* — Use to automatically configure the port.

7 AGGREGATING PORTS

This section contains information for configuring Link Aggregation, which optimizes port usage by linking a group of ports together to form a single *Link Aggregation Group (LAG).* An LAG aggregates ports into a single virtual port. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. Note the following:

- The device supports up to four LAGs, and eight ports in each LAG.
- The ports at both ends of a connection must be configured as trunk ports.
- Fast Ethernet ports and Gigabit Ethernet ports cannot be combined as members in a single trunk.
- All ports in a trunk assume the configuration settings of the first member port (that is, the first port assigned or the lowest numbered port if more than one port is assigned to a trunk in the same command), including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified LAG.
- Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the LAG's configuration settings are applied to the ports.

This section contains the following topics:

- Viewing Link Aggregation
- Configuring Link Aggregation
- Modifying Link Aggregation
- Removing Link Aggregation
- Viewing LACP
- Modifying LACP

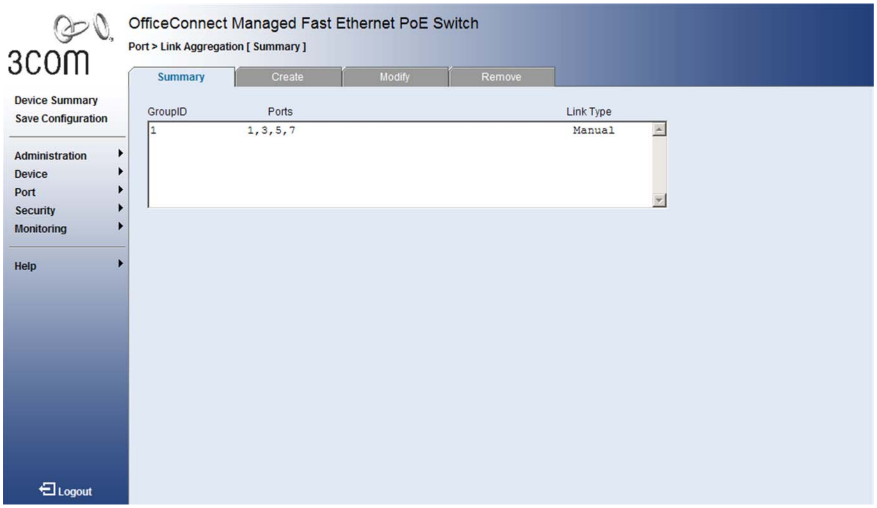
Viewing Link Aggregation

The *Link Aggregation Summary Page* displays the port members assigned to an LAG, and the method by which each LAG is formed.

To view Link Aggregation:

1 Click **Ports > Link Aggregation > Summary**. The *Link Aggregation Summary Page* opens:

Figure 61 Link Aggregation Summary Page



GroupID	Ports	Link Type
1	1,3,5,7	Manual

The *Link Aggregation Summary Page* includes the following fields:

- **Group ID** — Displays the Link Aggregated Group ID. The field range is *1-4*.
- **Ports** — Displays the member ports included in the specified LAG.
- **Link Type** — Displays the type of link aggregation used for the Group ID. The possible field values are *Manual* or *Dynamic*.

Configuring Link Aggregation

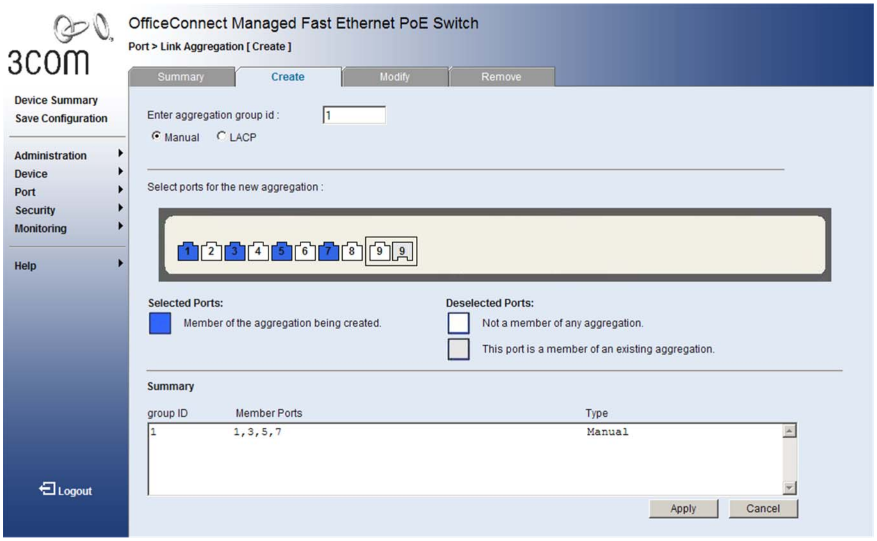
The *Link Aggregation Create Page* optimizes port usage by linking a group of ports together to form a single LAG.

Monitor users have no access to this page.

To create Link Aggregation:

1 Click **Ports > Link Aggregation > Create**. The *Link Aggregation Create Page* opens:

Figure 62 Link Aggregation Create Page



Enter aggregation group id : 1

● Manual ○ LACP

Select ports for the new aggregation :

Selected Ports:

🟦 Member of the aggregation being created.

Deselected Ports:

□ Not a member of any aggregation.

▨ This port is a member of an existing aggregation.

Summary

group ID	Member Ports	Type
1	1,3,5,7	Manual

The *Link Aggregation Create Page* includes the following fields:

- **Enter aggregation group ID** — Defines the group ID. The field range is *1-4*.
- **Manual** — Selects the link aggregation type to be static.
- **LACP** — Selects the link aggregation type to be LACP.
- **Select ports for the new aggregation** — Selects the ports for which the link aggregation parameters are to be defined. The ports are color-coded as follows:

  Selected ports

  - *Blue* — Displays a member of the aggregation being created.

Deselected ports

- *White* — Displays a non-existent member of any aggregation.
- *Grey* — Displays a member of an existing aggregation.

Summary

- **Group ID** — Displays the Link Aggregated Group ID. The field range is *1-4*.
- **Member Ports** — Displays the ports assigned to the link aggregation.
- **Type** — Displays the type of link aggregation. The possible field values are *Manual* or *Dynamic*.

2 Define the fields.

3 Click Apply. The link aggregation configuration is defined, and the device is updated.

Modifying Link Aggregation

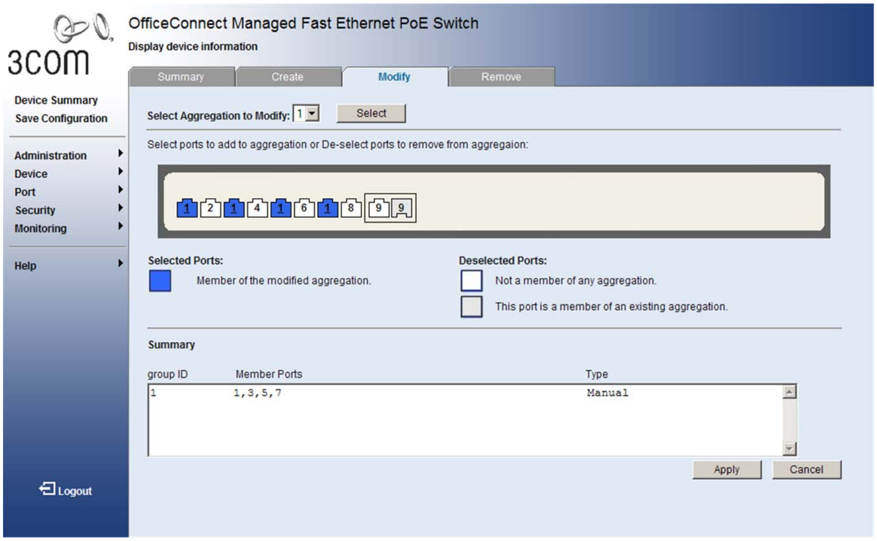
The *Link Aggregation Modify Page* allows you to change the member settings for an existing LAG.

Monitor users have no access to this page.

To modify Link Aggregation:

1 Click **Ports > Link Aggregation > Modify**. The *Link Aggregation Modify Page* opens:

Figure 63 Link Aggregation Modify Page



Select Aggregation to Modify: 1

Select ports to add to aggregation or De-select ports to remove from aggregaion:

Selected Ports:

🟦 Member of the modified aggregation.

Deselected Ports:

□ Not a member of any aggregation.

▨ This port is a member of an existing aggregation.

Summary

group ID	Member Ports	Type
1	1,3,5,7	Manual

The *Link Aggregation Modify Page* includes the following fields:

- **Select Aggregation to Modify** — Selects the Link Aggregation Group ID to modify.
- **Select ports to add to aggregation or de-select ports to remove from aggregation** — Allows the network manager to select ports to be added or removed from a current aggregation. The ports are color-coded as follows:

  Selected ports

  - *Blue* — Displays a member of the modified aggregation.

  Deselected ports

  - *White* — Not a member of any aggregation.
  - *Grey* — Displays a member of an existing aggregation.

Summary

- **Group ID** — Displays the Link Aggregated Group ID. The field range is *1-4*.
- **Member Ports** — Displays the ports configured to the link aggregation.
- **Type** — Displays the link aggregation type. The possible field values are *Manual* or *LACP*.

2 Define the fields.

3 Click Apply. The link aggregation modified, and the application is updated.

Removing Link Aggregation

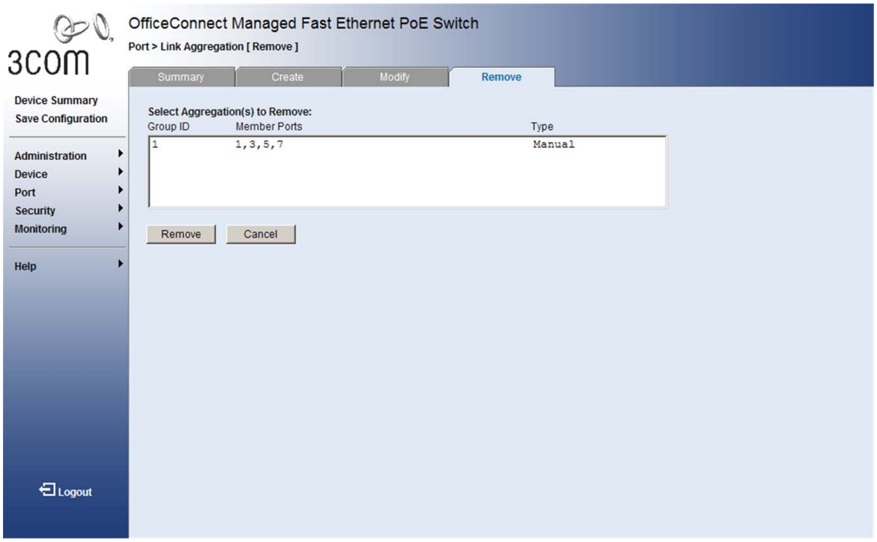
The *Link Aggregation Remove Page* allows the network manager to remove group IDs containing member ports.

Monitor users have no access to this page.

To remove Link Aggregation:

1 Click **Ports > Link Aggregation > Remove**. The *Link Aggregation Remove Page* opens:

Figure 64 Link Aggregation Remove Page



Select Aggregation(s) to Remove:

Group ID	Member Ports	Type
1	1,3,5,7	Manual

The *Link Aggregation Remove Page* includes the following fields:

- **Select Aggregation(s) to Remove** — Displays the Link Aggregation table. Allows selecting LAG IDs to be removed. Each row corresponds to a Link Aggregated Group ID. The fields in the table are:
  - *Group ID* — Displays the Link Aggregated Group ID. The field range is *1-4*.
  - *Member Ports* — Displays the ports for which the link aggregation parameters are defined.
  - *Type* — Displays the Link Aggregation type. The possible field values are *Manual* or *LACP*.

2 Select the group IDs to be removed

3 Click Remove. The link aggregations are removed, and the device is updated.

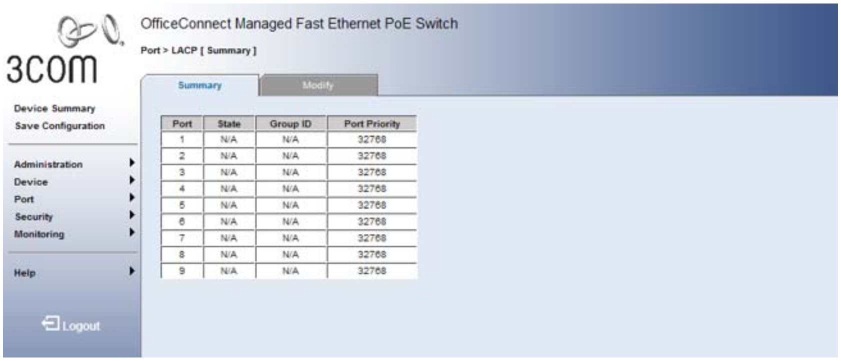
Viewing LACP

Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. The *LACP Summary Page* displays key information for each *Link Aggregation Group Protocol* (*LACP*) LAG.

To view LACP for LAGs:

1 Click **Port** > **LACP** > **Summary**. The *LACP Summary Page* opens:

Figure 65 LACP Summary Page



Port	State	Group ID	Port Priority
1	N/A	N/A	32768
2	N/A	N/A	32768
3	N/A	N/A	32768
4	N/A	N/A	32768
5	N/A	N/A	32768
6	N/A	N/A	32768
7	N/A	N/A	32768
8	N/A	N/A	32768
9	N/A	N/A	32768

The *LACP Summary Page* contains the following fields:

- **Port** — Displays the port number to which timeout and priority values are assigned.
- **State** — Displays the operational values of the actor's state parameters. The possible field values are N/A or Active.
- **Group ID** — Displays the Link Aggregated Group ID.
- **Port Priority** — Displays the LACP priority value for the port. The default is *1*. The field range is *1-65535*.

Modifying LACP

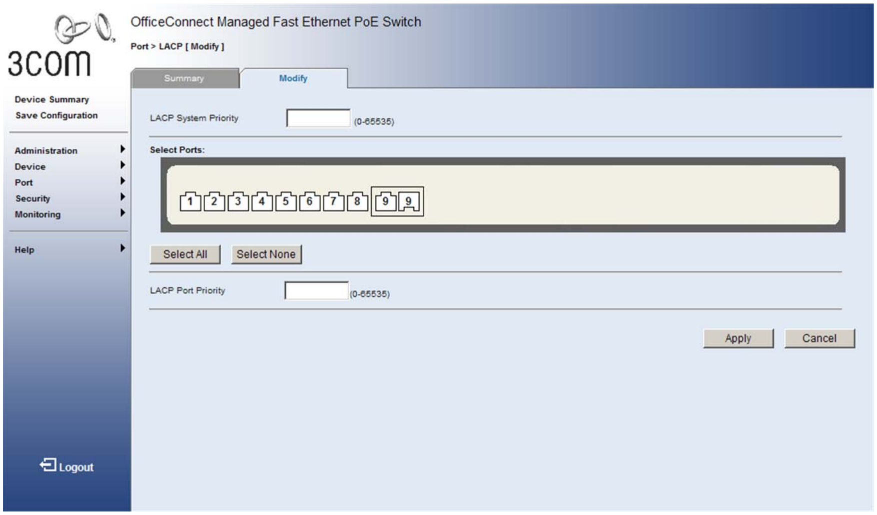
Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. The *LACP Modify Page* contains fields for modifying LACP system and port priority for LAGs.

Monitor users have no access to this page.

To modify LACP for LAGs:

1 Click **Port** > **LACP** > **Modify**. The *LACP Modify Page* opens:

Figure 66 LACP Modify Page



The *LACP Modify Page* contains the following fields:

- **LACP System Priority** — Specifies system priority value. Ports must be configured with the same system priority to join the same LAG. The default value is *32768*. The field range is *0-65535*.
- **Select Port** — Selects the port number to which timeout and priority values are assigned.
- **LACP Port Priority** — Specifies the LACP priority value for the port. If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. The default is *32768*. The field range is *0-65535*.

2 Define the fields.

3 Click Apply. The LACP Link Aggregation is modified, and the application is updated.

8 CONFIGURING VLANS

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented. VLANs restrict traffic within the VLAN.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN 1is the default VLAN. All ports are members of VLAN 1 by default. If the untagged port is moved to a new VLAN, the port is removed from VLAN 1. For example: If an untagged port 24 is moved to VLAN 5, the port will no longer be a member of VLAN 1. However, if the port is added to VLAN 5 as a tagged port it then remains untagged in VLAN 1.

This section contains the following topics:

- Viewing VLAN Details
- Viewing VLAN Port Details
- Creating VLANs
- Renaming VLANs
- Modifying VLAN Settings
- Modifying Port VLAN Settings
- Removing VLANs

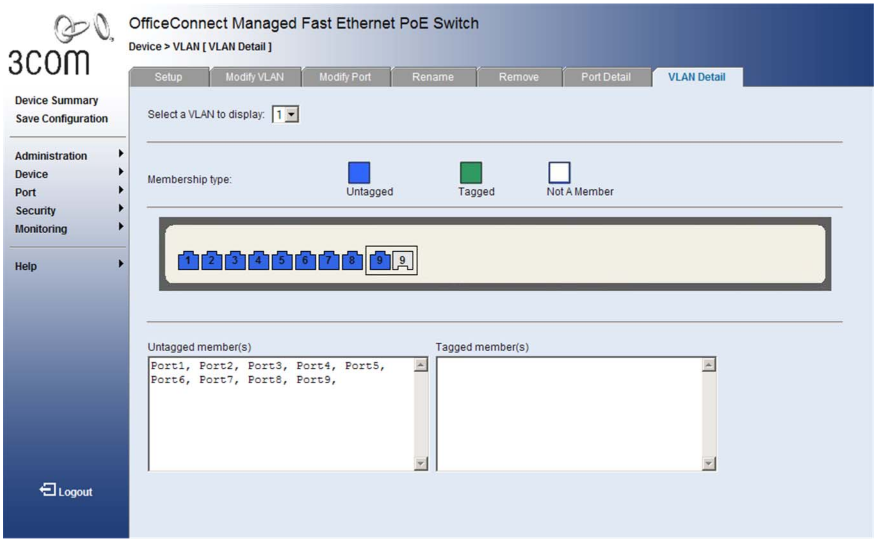
Viewing VLAN Details

The *VLAN Detail Page* provides information and global parameters on VLANs configured on the system.

To view VLAN details:

1 Click **Device > VLAN > VLAN Detail**. The *VLAN Detail Page* opens:

Figure 67 VLAN Detail Page



Select a VLAN to display: 1

Membership type: Untagged Tagged Not A Member

Untagged member(s)

```
Port1, Port2, Port3, Port4, Port5,
Port6, Port7, Port8, Port9,
```

Tagged member(s)

The *VLAN Detail Page* contains the following information:

- **Select a VLAN to display**— Selects a VLAN to be display its settings.
- **Membership type** — Displays the membership type for each VLAN. The possible field values are:
  - *Untagged* — Indicates the interface is an untagged member of the VLAN.
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. VLAN tagged frames are forwarded by the interface. The frames contain VLAN information.
  - *Not A Member* — Indicates the interface is not a member of the VLAN

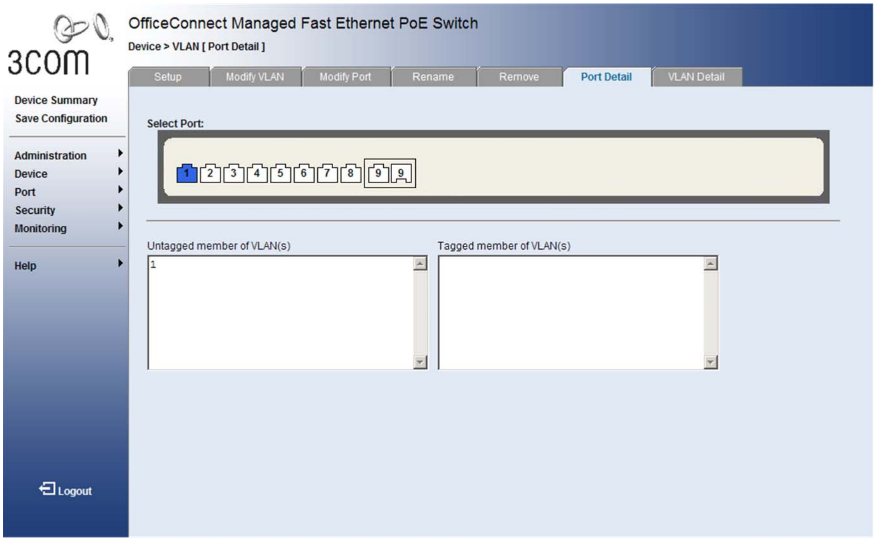
Viewing VLAN Port Details

The *VLAN Port Detail Page* provides information on VLAN configured ports.

To view VLAN Port details:

1 Click **Device > VLAN > Port Detail**. The *VLAN Port Detail Page* opens:

Figure 68 VLAN Port Detail Page



Untagged member of VLAN(s)

1

Tagged member of VLAN(s)

The *VLAN Port Detail Page* contains the following information:

- **Select Port** — Selects the ports to be displayed.
- **Untagged member of VLAN(s)** — Indicates the port is an untagged member of the VLAN.
- **Tagged ember of VLAN(s)** — Indicates the port is a tagged member of a VLAN. VLAN tagged frames are forwarded by the interface. The frames contain VLAN information.

Creating VLANs

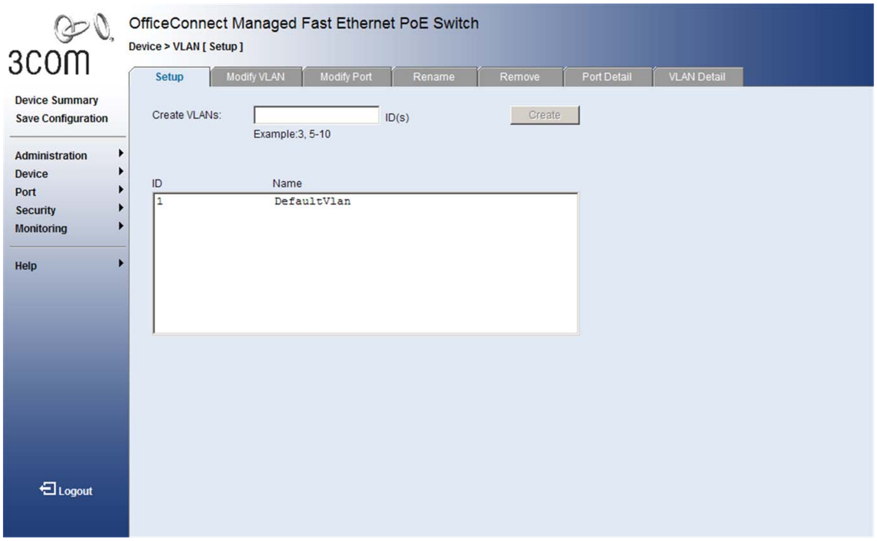
The *VLAN Setup Page* allows the network administrator to create or rename VLANs.

Monitor users have no access to this page.

To create VLANs:

1 Click **Device > VLAN > Setup**. The *VLAN Setup Page* opens:

Figure 69 VLAN Setup Page



Create VLANs: ID(s)
Example:3, 5-10

ID	Name
1	DefaultVlan

The *VLAN Setup Page* contains the following fields:

Create VLANs

- **ID(s)** — Defines the VLAN ID(s) to create.
- **Create** — Creates the VLAN ID(s).

VLAN List

- **ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.

2 Enter the VLAN ID number(s).

3 Click Create. The VLAN(s) are created, and the device is updated.

Renaming VLANs

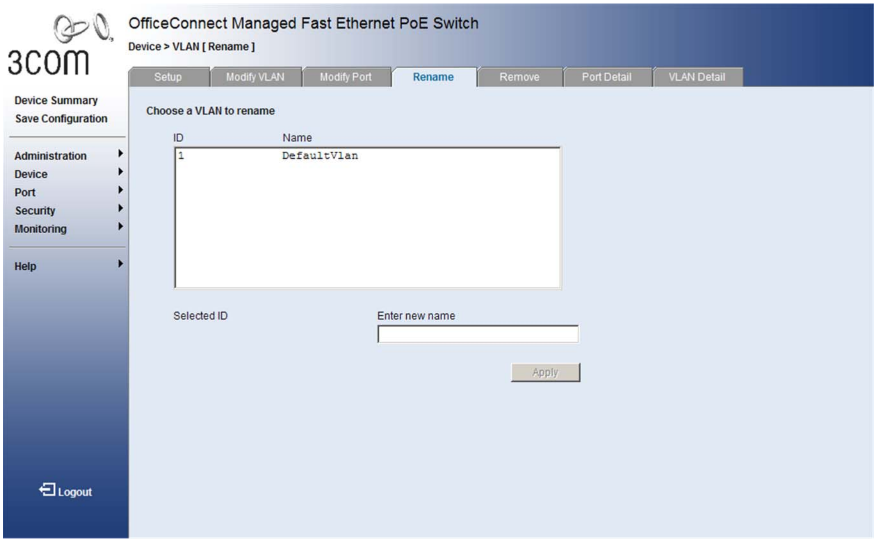
The *VLAN Rename Page* allows the network administrator to rename VLANs.

Monitor users have no access to this page.

To rename VLANs:

1 Click **Device > VLAN > Rename**. The *VLAN Rename Page* opens:

Figure 70 VLAN Rename Page



Choose a VLAN to rename

ID	Name
1	DefaultVlan

Selected ID

Enter new name

The *VLAN Rename Page* contains the following fields:

- **ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.
- **Selected ID** — ID of entry selected from list of configured VLANs.
- **Enter new name** — New name for the selected entry.

To rename a VLAN:

1 Highlight a VLAN to be renamed from the VLAN list.

2 Enter the new name for the VLAN.

3 Click Apply. The VLAN is renamed, and the device is updated.

Modifying VLAN Settings

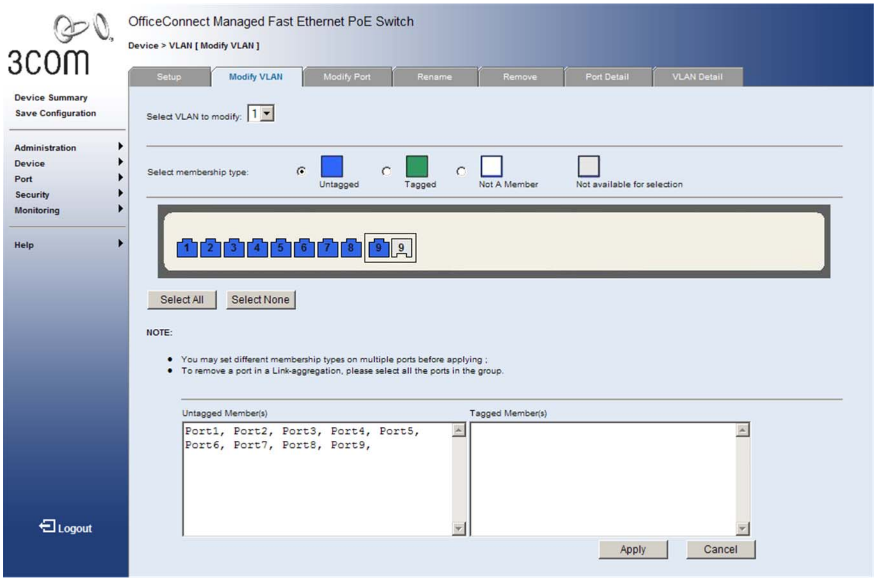
The *Modify VLAN Page* allows the network manager to change VLAN membership.

Monitor users have no access to this page.

To edit VLAN Settings:

Click **Device > VLAN > Modify VLAN**. The *Modify VLAN Page* opens:

Figure 71 Modify VLAN Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > VLAN [Modify VLAN]

Select VLAN to modify: 1

Select membership type: ● Untagged ○ Tagged ○ Not A Member

NOTE:

- You may set different membership types on multiple ports before applying ;
- To remove a port in a Link-aggregation, please select all the ports in the group.

Untagged Member(s): Port1, Port2, Port3, Port4, Port5, Port6, Port7, Port8, Port9,

Tagged Member(s):

The *Modify VLAN Page* contains the following fields:

- **Select a VLAN to modify** — Selects a VLAN to modify its settings.
- **Select membership type** — Selects the membership type for each port on the VLAN. The possible field values are:
  - *Untagged* — Indicates the interface is an untagged member of the VLAN.
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. VLAN tagged frames are forwarded by the interface. The frames contain VLAN information.
  - *Not A Member* — Indicates the interface is not a member of the VLAN.

  - *Not available for selection* — Indicates the interface is not available for selection.
- **Select All** — Allows you to select all ports to be added to the VLAN.
- **Select None** — Removes the ports selected.

To add ports to a VLAN

1 Select a VLAN to modify.

2 Select the membership type for the selected ports.

3 Select ports to be added to the selected VLAN.

4 You may select different membership types on multiple ports by repeating step 2 and step 3.

5 Click Apply. The selected ports are added to the VLAN, and the device is updated.

Modifying Port VLAN Settings

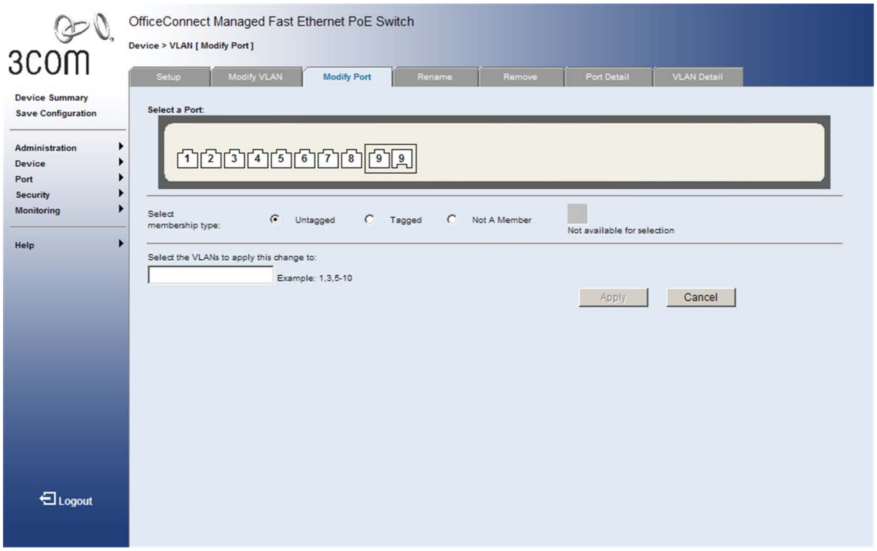
The *Modify Port Page* allows the network manager to modify port VLAN settings.

Monitor users have no access to this page.

To modify Port VLAN Settings:

1 Click **Device > VLAN > Modify Port**. The *Modify Port Page* opens:

Figure 72 Modify Port Page



Select a Port:

Select membership type: ● Untagged ○ Tagged ○ Not A Member ▨ Not available for selection

Select the VLANs to apply this change to: Example: 1,3,5-10

The *Modify Port Page* contains the following fields:

- **Select a Port** — Selects a port to be modified.
- **Select membership type** — Displays the membership type for each port on the VLAN. The possible field values are:
  - *Untagged* — Indicates the interface is an untagged member of the VLAN.
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. VLAN tagged frames are forwarded by the interface. The frames contain VLAN information.
  - *Not A Member* — Indicates the interface is not a member of the VLAN.
  - *Not available for selection* — Indicates the interface is not available for selection.

- *Select the VLANs to apply this change to* — Defines the VLAN ID to which the port is to be assigned.

2 Select a port.

3 Select the port’s membership type.

4 Enter the VLAN ID to be assigned to the port.

5 Click Apply . The VLANs are configured, and the device is updated.

Removing VLANs

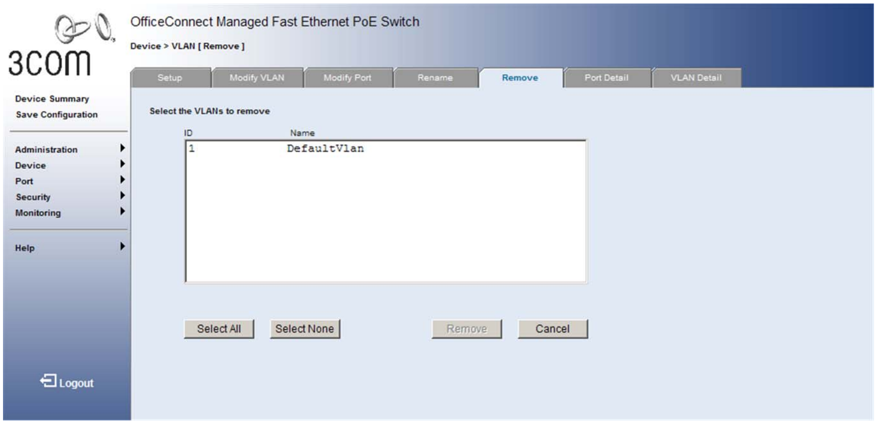
The *VLAN Remove Page* allows the network administrator to remove VLANs.

Monitor users have no access to this page.

To delete VLANs:

1 Click **Device > VLAN > Remove**. The *VLAN Remove Page* opens:

Figure 73 VLAN Remove Page



Select the VLANs to remove

ID	Name
1	DefaultVlan

The *VLAN Remove Page* contains the following fields:

- **ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.
- **Select All** — Allows the user to select the entire table to be removed.
- **Select None** — Deselects all entries in the VLAN list.

2 Select the VLAN IDs to be deleted.

3 Click Remove . The selected VLANs are deleted, and the device is updated.

9 Configuring IP and MAC Address Information

This section contains information for defining IP interfaces, and includes the following sections:

- Defining IP Addressing
- Configuring ARP Settings
- Viewing Address Tables

Defining IP Addressing

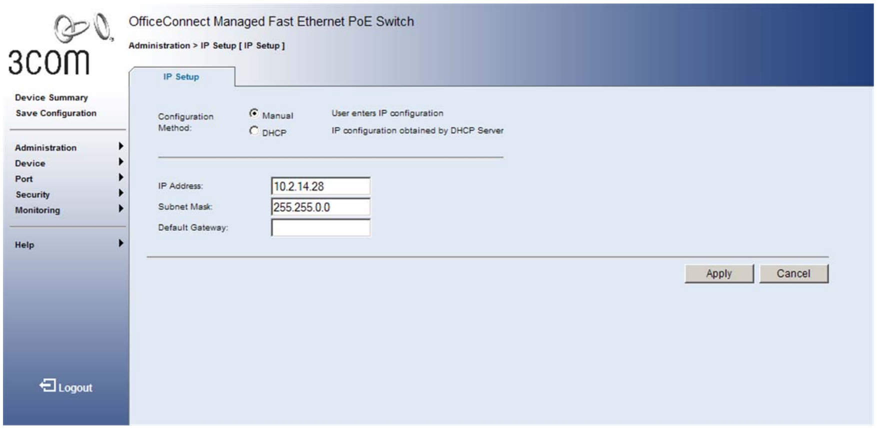
The *IP Setup Page* contains fields for assigning an IP address. The Default Gateway is erased when the IP Address is modified and changed. Packets are forwarded to the default gateway when sent to a remote network.

Monitor user has no access to this page.

To define an IP interface:

1 Click **Administration > IP Setup**. The *IP Setup Page* opens:

Figure 74 IP Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Administration > IP Setup [IP Setup]

Configuration Method: ● Manual — User enters IP configuration; ○ DHCP — IP configuration obtained by DHCP Server

IP Address: 10.2.14.28

Subnet Mask: 255.255.0.0

Default Gateway:

The *IP Setup Page* contains the following fields:

- **Configuration Method** — Defines whether the IP address is configured statically or dynamically. The possible field values are:
  - *Manual* — Specifies that the IP Interface is configured by the user.
  - *DHCP* — Specifies that the IP Interface is dynamically created.
- **IP Address** — Defines the IP address.
- **Subnet Mask** — Defines the subnet mask.
- **Default Gateway** — Defines the default gateway.

2 Select *Manual* or *DHCP* mode.

3 If *Manual* is selected, configure the *IP Address, Subnet Mask* and *Default Gateway.*

4 Click Apply. The IP configuration is enabled, and the device is updated.

Configuring ARP Settings

The *Address Resolution Protocol* (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts when only the IP address of its neighbors is known.

This section includes the following sections:

- Viewing ARP Settings
- Defining ARP Settings
- Removing ARP Entries

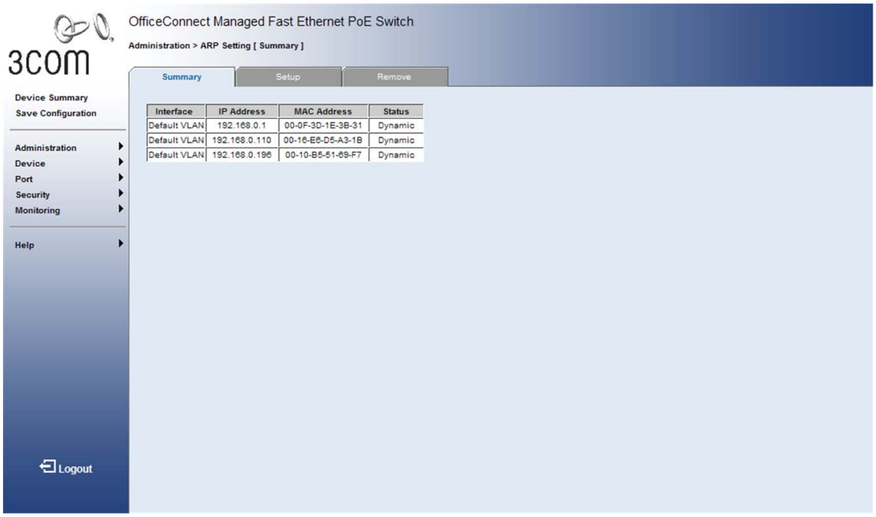
Viewing ARP Settings

The *ARP Settings Summary Page* displays the current ARP settings.

To view ARP Settings:

1 Click **Administration > ARP Settings > Summary**. The *ARP Settings Summary Page* opens:

Figure 75 ARP Settings Summary Page



Interface	IP Address	MAC Address	Status
Default VLAN	192.168.0.1	00-0F-3D-1E-3B-31	Dynamic
Default VLAN	192.168.0.110	00-16-E6-D5-A3-1B	Dynamic
Default VLAN	192.168.0.196	00-10-B5-51-69-F7	Dynamic

The *ARP Settings Summary Page* contains the following fields:

- **Interface** — Indicates the VLAN for which ARP parameters are defined.
- **IP Address** — Indicates the station IP address, which is associated with the MAC Address.
- **MAC Address** — Displays the station MAC address, which is associated in the ARP table with the IP address.
- **Status**— Displays the ARP table entry type. Possible field values are:
  - *Dynamic* — Indicates the ARP entry is learned dynamically.
  - *Static* — Indicates the ARP entry is a static entry.

Defining ARP Settings

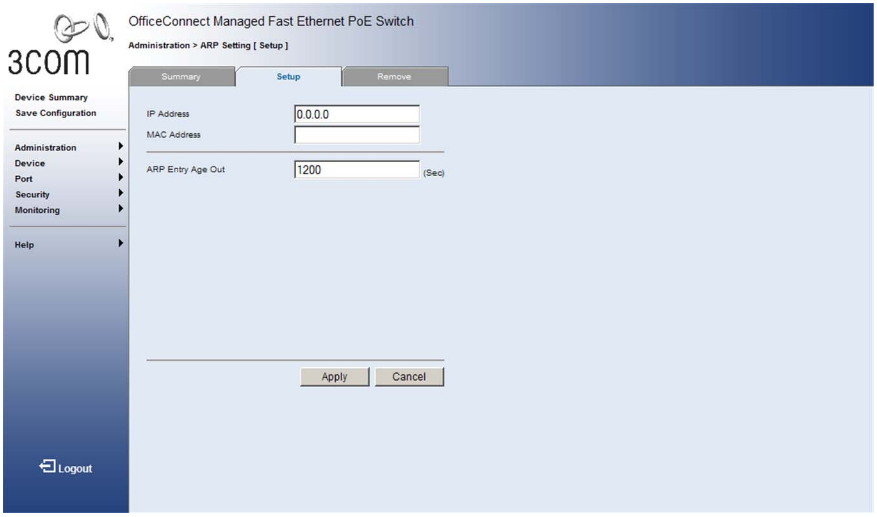
The *ARP Settings Setup Page* allows network managers to define ARP parameters for specific interfaces.

Monitor users have no access to this page.

To configure ARP entries:

1 Click **Administration > ARP Settings > Setup**. The *ARP Settings Setup Page* opens:

Figure 76 ARP Settings Setup Page



IP Address 0.0.0.0
MAC Address
ARP Entry Age Out 1200 (Sec)

The *ARP Settings Setup Page* contains the following fields:

- **IP Address**— Defines the station IP address, which is associated with the MAC address. Note that this address must be within the same IP subnet as that assigned to the switch (see *Defining IP Addressing* on page 142).
- **MAC Address** — Defines the station MAC address, which is associated in the ARP table with the IP address.
- **ARP Entry Age Out** — Specifies the amount of time (in seconds) that passes between ARP Table entry requests. Following the *ARP Entry Age* period, the entry is deleted from the table. The range is *1-86400* seconds. The default value is *1200* seconds.

2 Define the fields.

3 Click Apply. The ARP parameters are defined, and the device is updated.

Removing ARP Entries

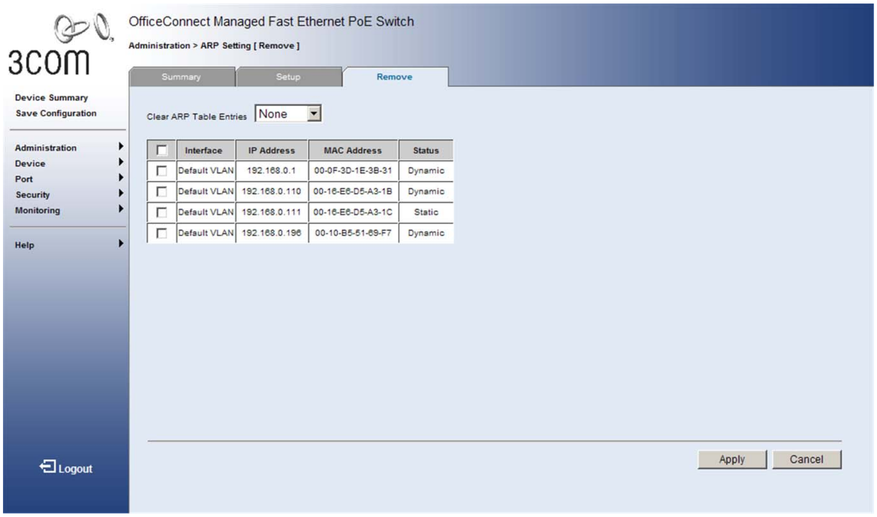
The *ARP Settings Remove Page* provides parameters for removing ARP entries from the ARP Table.

Monitor user has no access to this page.

To remove ARP entries:

1 Click **Administration > ARP Settings > Remove**. The *ARP Settings Remove Page* opens:

Figure 77 ARP Settings Remove Page



Clear ARP Table Entries: None

□	Interface	IP Address	MAC Address	Status
□	Default VLAN	192.168.0.1	00-0F-3D-1E-3B-31	Dynamic
□	Default VLAN	192.168.0.110	00-16-E6-D5-A3-1B	Dynamic
□	Default VLAN	192.168.0.111	00-16-E6-D5-A3-1C	Static
□	Default VLAN	192.168.0.196	00-10-B5-51-69-F7	Dynamic

The *ARP Settings Remove Page* contains the following fields:

- **Clear ARP Table Entries** — Specifies the types of ARP entries that are cleared. The possible values are:
  - *None* — Maintains the ARP entries.
  - *All* — Clears all ARP entries.
  - *Dynamic* — Clears only dynamic ARP entries.
  - *Static* — Clears only static ARP entries.
- Checkbox (unnamed) — Selects the ARP entry for removal.
- **Interface** — Indicates the VLAN for which ARP parameters are defined.
- **IP Address** — Indicates the station IP address which is associated with the MAC address.

- **MAC Address** — Displays the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Displays the ARP table entry type. Possible field values are:
  - *Dynamic* — Indicates the ARP entry is learned dynamically.
  - *Static* — Indicates the ARP entry is a static entry.

2 For each ARP entry to be removed, check the box to the left of the row in the table. To remove all ARP entries, the topmost box may be checked.

3 Click Remove. The ARP table entries are removed, and the device is updated.

Viewing Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address database. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. MAC addresses are dynamically learned as packets arrive at the device. Addresses are associated with ports by learning the ports from the frames source address. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

This section includes the following sections:

- Viewing Address Table Settings
- Viewing Port Summary Settings

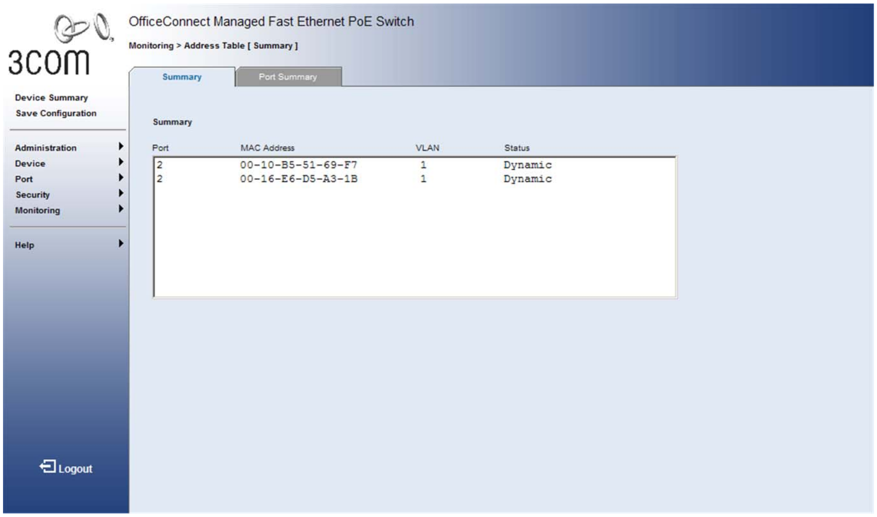
Viewing Address Table Settings

The *Address Table Summary Page* displays the current MAC address table configuration.

To view address table settings:

1 Click **Monitoring > Address Table > Summary**. The *Address Table Summary Page* opens:

Figure 78 Address Table Summary Page



Summary

Port	MAC Address	VLAN	Status
2	00-10-B5-51-69-F7	1	Dynamic
2	00-16-E6-D5-A3-1B	1	Dynamic

The *Address Table Summary Page* contains the following fields:

- **Port** — Indicates the port through which the address was learned.
- **MAC Address** — Displays the current MAC addresses listed in the MAC address table.
- **VLAN** — Displays the VLAN ID associated with the port and MAC address.
- **Status** — Displays the MAC address entry type. Possible values are:
  - *Dynamic* — Indicates the MAC address is learned dynamically.
  - *Static* — Indicates the MAC address is statically configured.

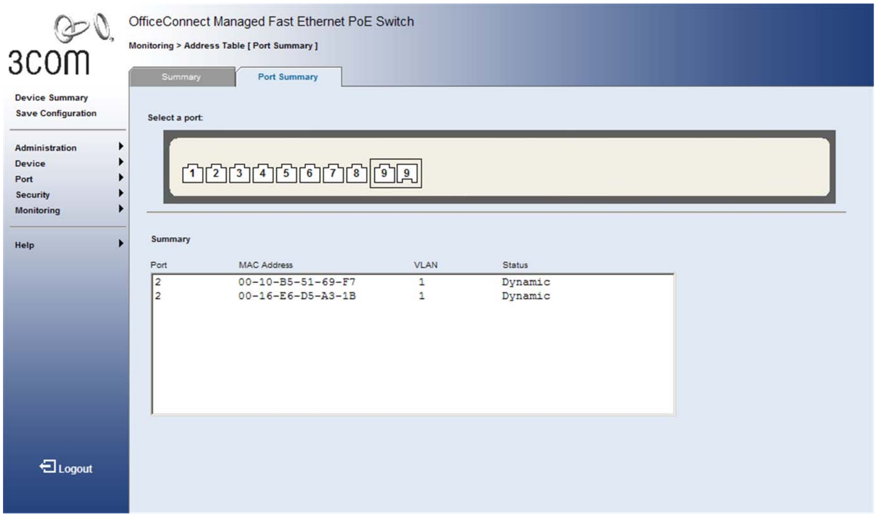
Viewing Port Summary Settings

The *Port Summary Page* allows the user to view the MAC addresses assigned to specific ports.

To view Port Summary settings:

1 Click **Monitoring > Address Table > Port Summary**. The *Port Summary Page* opens:

Figure 79 Port Summary Page



Port	MAC Address	VLAN	Status
2	00-10-B5-51-69-F7	1	Dynamic
2	00-16-E6-D5-A3-1B	1	Dynamic

The *Port Summary Page* contains the following fields:

- **Select a port** — Displays the current port settings.
- **Port** — Indicates the port through which the address was learned.
- **MAC Address** — Displays MAC addresses currently listed in the MAC address table.
- **VLAN** — Displays the VLAN ID associated with the port and MAC address.
- **Status** — Displays the MAC address configuration method. Possible values are:
  - *Dynamic* — Indicates the MAC address is learned dynamically.
  - *Static* — Indicates the MAC address is statically configured.

10 CONFIGURING IGMP SNOOPING

This section contains information for configuring IGMP Snooping and IGMP Query.

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

If IGMP Query is enabled and this switch is elected as the querier for the local LAN segment, it will periodically poll each known multicast group for active members, and dynamically configure the switch ports which need to forward multicast traffic. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

This section contains the following topic:

- Defining IGMP Snooping and Query

Defining IGMP Snooping and Query

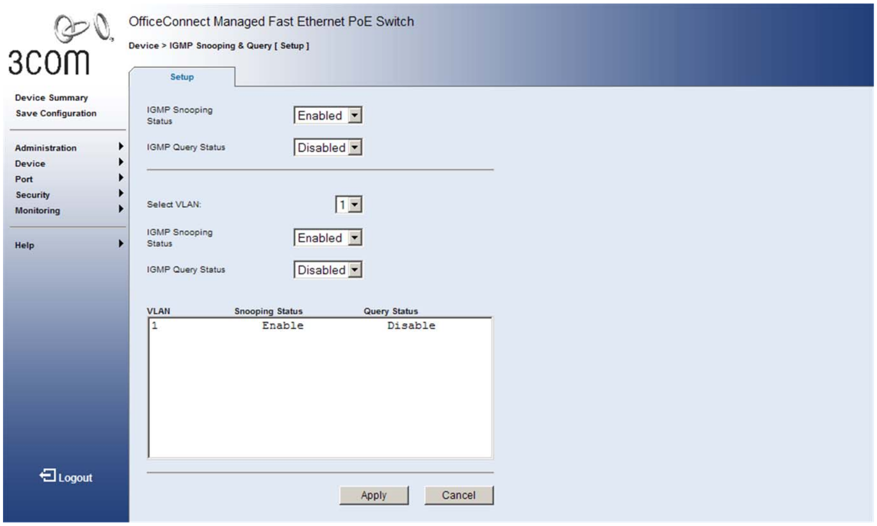
The *IGMP Snooping and Query Setup Page* allows network managers to define IGMP Snooping and Query parameters for VLANs.

Monitor users have no access to this page.

To configure IGMP Snooping:

Click **Device > IGMP Snooping > Setup**. The *IGMP Snooping and Query Setup Page* opens:

Figure 80 IGMP Snooping and Query Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > IGMP Snooping & Query [Setup]

IGMP Snooping Status: Enabled

IGMP Query Status: Disabled

Select VLAN: 1

IGMP Snooping Status: Enabled

IGMP Query Status: Disabled

VLAN	Snooping Status	Query Status
1	Enable	Disable

The *IGMP Snooping and Query Setup Page* contains the following fields:

Global Settings

- **IGMP Snooping Status** — Defines whether IGMP Snooping is enabled on the device. The possible field values are:
  - *Disabled* — Indicates that IGMP Snooping is disabled on the device.
  - *Enabled* — Indicates that IGMP Snooping is enabled on the device. This is the default value.

- **IGMP Query Status** — Defines whether IGMP Query is enabled on the device. The possible field values are:
    - *Disabled* — Indicates that IGMP Query is disabled on the device. This is the default value.
    - *Enabled* — Indicates that IGMP Query is enabled on the device.

VLAN Settings

- **Select VLAN** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Defines whether IGMP snooping is enabled on the VLAN. The possible field values are:
    - *Disabled* — Disables IGMP Snooping on the VLAN.
    - *Enabled* — Enables IGMP Snooping on the VLAN. This is the default value.
- **IGMP Query Status** — Defines whether IGMP Query is enabled on the VLAN. The possible field values are:
    - *Disabled* — Disables IGMP Query on the VLAN. This is the default value.
    - *Enabled* — Enables IGMP Query on the VLAN.

VLAN Summary

- **VLAN** — Displays the VLAN ID.
- **Snooping Status** — Displays the IGMP snooping status for the VLAN. The possible field values are *Enabled* and *Disabled*.
- **Query Status** — Displays the IGMP query status for the VLAN. The possible field values are *Enabled* and *Disabled*.

To enable or disable IGMP Snooping or IGMP Query on the device:

1. Select *Enable* or *Disable* from the *IGMP Snooping Status* or *IGMP Query Status* list.
2. Click Apply. IGMP Snooping and IGMP Query is enabled or disabled on the device, and the device is updated.

To enable or disable IGMP Snooping or IGMP Query on a selected VLAN:

1. Enable IGMP Snooping or IGMP Query on the device.
2. Select the VLAN ID from the *Select VLAN* list.
3. Select *Enable* or *Disable* from the *IGMP Snooping Status* or *IGMP Query Status* list.

4 Click Apply. IGMP Snooping and IGMP Query is enabled or disabled on the VLAN, and the device is updated.

11 CONFIGURING SPANNING TREE

This section contains information for configuring the Spanning Tree Algorithm (STA). This algorithm provides a tree topography for any arrangement of bridges. It also provides a single path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reduced network efficiency.

The device supports the following STA versions:

- *Spanning Tree Protocol* (STP, IEEE 802.1D) — This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.
- *Rapid Spanning Tree Protocol* (RSTP, IEEE 802.1w) — This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the STP protocol, by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

This section contains the following topics:

- Viewing Spanning Tree
- Defining Global Settings for Spanning Tree
- Defining Port Settings for Spanning Tree

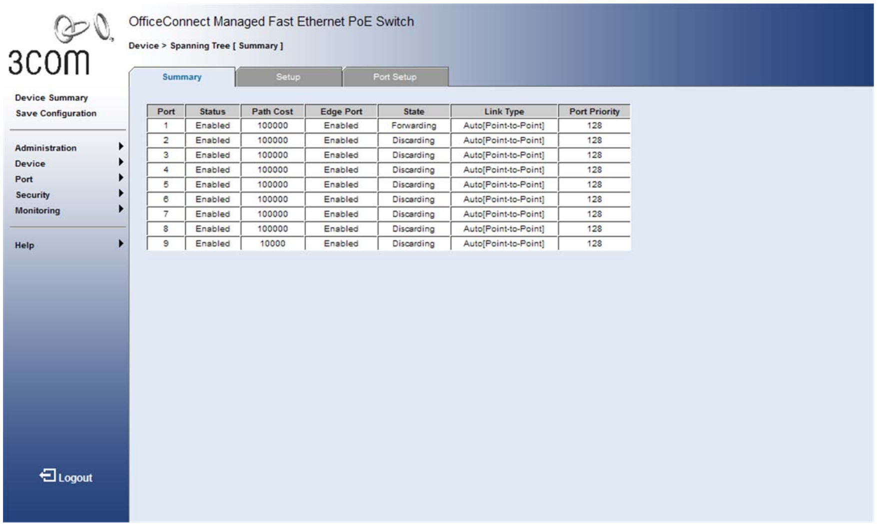
Viewing Spanning Tree

The *Spanning Tree Summary Page* displays the current Spanning Tree parameters for all ports.

To view Spanning Tree Summary:

1 Click **Device > Spanning Tree > Summary**. The *Spanning Tree Summary Page* opens:

Figure 81 Spanning Tree Summary Page



Port	Status	Path Cost	Edge Port	State	Link Type	Port Priority
1	Enabled	100000	Enabled	Forwarding	Auto[Point-to-Point]	128
2	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
3	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
4	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
5	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
6	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
7	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
8	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
9	Enabled	10000	Enabled	Discarding	Auto[Point-to-Point]	128

The *Spanning Tree Summary Page* contains the following fields:

- **Port** — Indicates the interface for which the information is displayed.
- **Status** — Indicates if STA is enabled on the port. The possible field values are:
  - *Enabled* — Indicates that STA is enabled on the port.
  - *Disabled* — Indicates that STA is disabled on the port.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost can be adjusted to a higher or lower value, and is used to determine the path used to forward traffic when a path is re-routed.
- **Edge Port** — Indicates if fast forwarding is enabled on the port. If enabled, the port is automatically placed in the *Forwarding* state when the port link is up. Edge Port optimizes STA protocol topology convergence, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to

reconfigure when the interface changes state, and also overcomes other STA-related timeout problems.

- **State** — Displays the current STA state of a port. If enabled, the port state determines what action is taken on traffic. Possible port states are:
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
  - *Discarding* — Indicates that the port is in Discarding mode. The port is listening to BPDUs, and discards any other frames it receives.
- **Link Type** — Indicates the established link type. The possible field values are:
  - *Auto* — Automatically derived from the duplex mode setting. Ports set to full duplex mode are considered Point-to-Point port links, while ports set to half-duplex mode are assumed to be on a shared link.
  - *Point to Point* — Indicates that a point-to-point link is currently established on the port.
  - *Shared* — Indicates that a shared link is currently established on the port.
- **Port Priority** — Indicates the priority value of the port. The priority influences the port choice when a bridge has two ports connected in a loop. If the path cost for all ports on a switch is the same, the port with the highest priority will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops.

Defining Global Settings for Spanning Tree

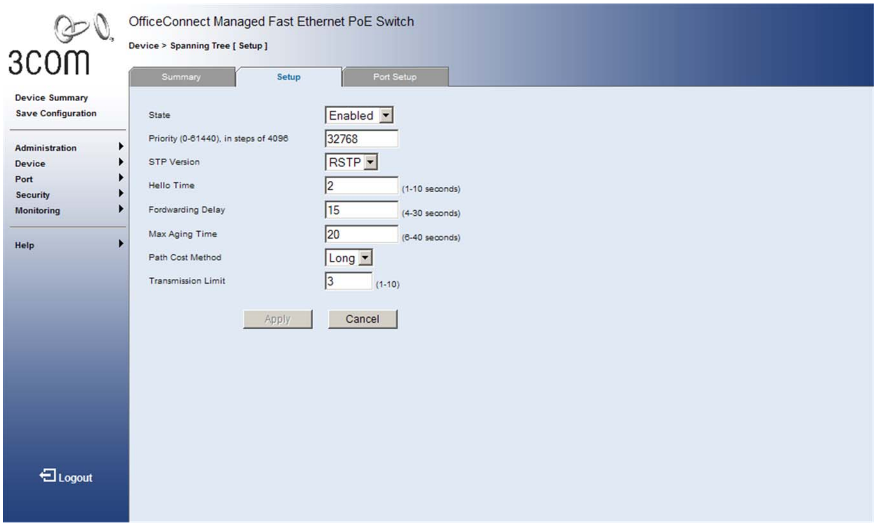
Network administrators can assign STA settings to specific interfaces using the *Spanning Tree Setup Page*.

Monitor users have no access to this page.

To configure Spanning Tree Setup:

1 Click **Device > Spanning Tree > Setup**. The *Spanning Tree Setup Page* opens:

Figure 82 Spanning Tree Setup Page



State: Enabled

Priority (0-61440), in steps of 4096: 32768

STP Version: RSTP

Hello Time: 2 (1-10 seconds)

Fordwarding Delay: 15 (4-30 seconds)

Max Aging Time: 20 (6-40 seconds)

Path Cost Method: Long

Transmission Limit: 3 (1-10)

The *Spanning Tree Setup Page* contains the following fields:

- **State** — Defines whether STA is enabled or disabled on the device. The possible field values are:
  - *Disabled* — Disables STP and RSTP on the device.
  - *Enabled* — Enables STP or RSTP on the device.
- **Priority** — Specifies the bridge priority value. When switches or bridges are running STA, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The field range is *0-61440*. The default value is *32768*. The priority value is provided in increments of 4096.

- **STP Version** — Defines whether STP or RSTP is enabled on the device. The possible field values are:.
  - *RSTP* — Enables RSTP on the device.
  - *STP* — Enables STP on the device.
- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root Bridge waits between configuration messages. The default is 2 seconds.
- **Forwarding Delay** — Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.
- **Max Aging Time** — Specifies the device Maximum Age Time. The Maximum Age Time is the amount of time in seconds a bridge waits before sending configuration messages. The default is 20 seconds.
- **Path Cost Method** — Specifies the method used to assign default path cost to STA ports. The possible field values are:
  - *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
  - *Long* — Specifies 1 through 200,000,000 range for port path cost. The default path cost assigned to an interface varies according to the selected method (*Hello Time*, *Max Age*, or *Forward Delay*).
- **Transmission Limit** — Specifies the minimum interval between the transmission of consecutive RSTP BPDUs. The default is 3 seconds.

2 Define the fields.

3 Click Apply. STA is configured, and the device is updated.

Defining Port Settings for Spanning Tree

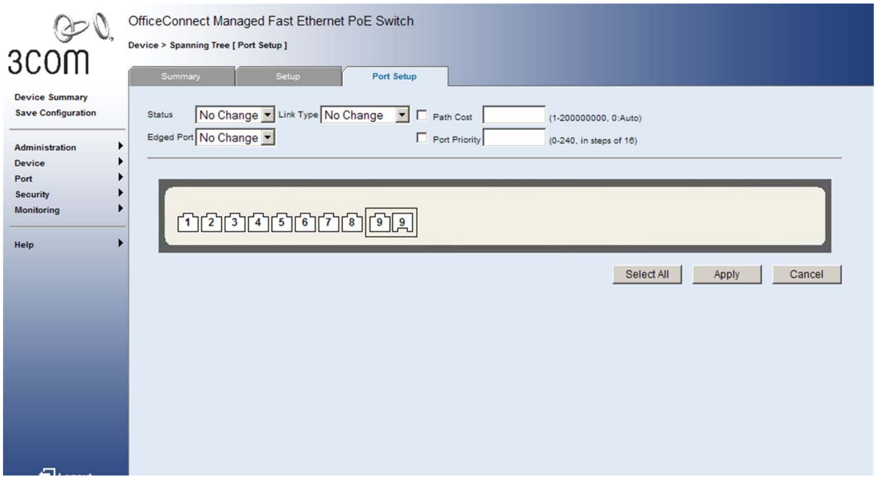
The *Spanning Tree Port Setup Page* contains information for modifying Spanning Tree parameters.

Monitor users have no access to this page.

To modify Spanning Tree:

1 Click **Device > Spanning Tree > Port Setup**. The *Spanning Tree Port Setup Page* opens:

Figure 83 Spanning Tree Port Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > Spanning Tree [Port Setup]

Status: No Change | Link Type: No Change | □ Path Cost: (1-200000000, 0:Auto)

Edged Port: No Change | □ Port Priority: (0-240, in steps of 16)

The *Spanning Tree Port Setup Page* contains the following fields:

- **Status** — Specifies if STA is enabled on the port. The possible field values are:
  - *Enabled* — Indicates that STA is enabled on the port.
  - *Disabled* — Indicates that STA is disabled on the port.
- **Edge Port** — Specifies if fast forwarding is enabled on the port. If enabled, the port is automatically placed in the *Forwarding* state when the port link is up. Edge Port optimizes STA protocol topology convergence, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. The possible field values are:
  - *Enabled* — Enables edge port on the port.
  - *Disabled* — Disables edge port on the port.

- **Link Type** — Specifies the link type. The possible field values are:
  - *Auto* — Automatically derived from the duplex mode setting. Ports set to full duplex mode are considered Point-to-Point port links, while ports set to half-duplex mode are assumed to be on a shared link.
  - *Point to Point* — Configures a point-to-point link on the port. Specify a point-to-point link if the port can only be connected to exactly one other bridge.
  - *Shared* — Configures a shared link on the port. Specify a shared link if the port can be connected to two or more bridges.
- **Path Cost** — Defines the port contribution to the root path cost. The path cost can be adjusted to a higher or lower value, and is used to determine the path used to forward traffic when a path is re-routed. The field range is 1-200,000,000 for the long path cost method and 1-65,535 for the short path cost method.

Table 10 Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

The system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below for IEEE 802.1w. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 11 Default STA Path Cost

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex	4	10,000

Path Cost is used by the Spanning Tree Algorithm 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.

Path cost takes precedence over port priority.

- **Priority** — Defines the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between *0-240*. The priority value is determined in increments of 16.

  If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

  Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

2. Select the ports to be defined
3. Define the fields.
4. Click Apply. Spanning Tree is modified on the port, and the device is updated.

12 CONFIGURING SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP version 1
- SNMP version 2c

SNMP v1 and v2c

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

This section contains the following topics:

- Setting SNMP Agent Status
- Defining SNMP Communities and Traps
- Removing SNMP Communities or Traps

Setting SNMP Agent Status

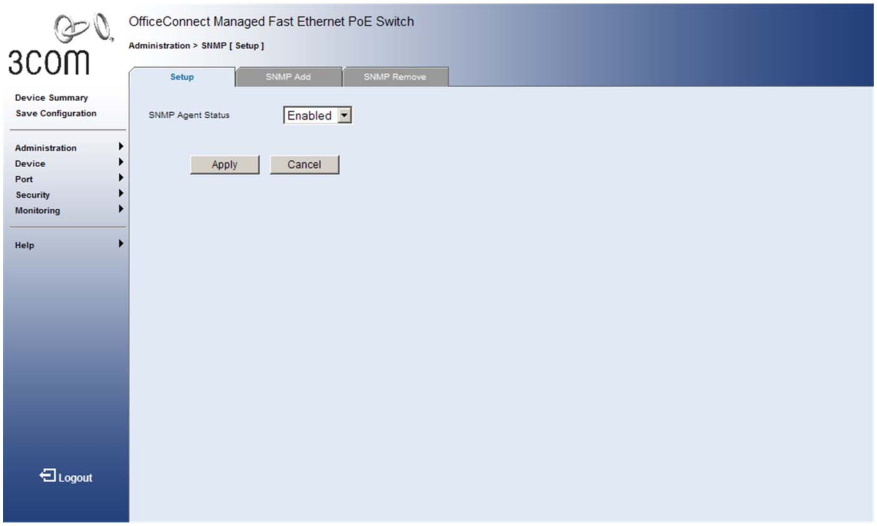
SNMP services can be enabled or disabled for all management clients (that is, versions 1 and 2c) using the *SNMP Setup Page*.

Monitor users have no access to this page.

To set the operational status for SNMP:

1 Click **Administration > SNMP > Setup**. The *SNMP Setup Page* opens:

Figure 84 SNMP Setup Page



SNMP Agent Status: Enabled

The *SNMP Setup Page* contains the following fields:

- **SNMP Agent Status** — Specifies if SNMP is enabled on the device. The possible field values are:
  - *Enabled* — Enables SNMP on the device.
  - *Disabled* — Disables SNMP on the device.

2 Set the status field.

3 Click Apply. The SNMP agent status is defined, and the device is updated.

Defining SNMP Communities and Traps

Access rights are managed by defining communities in the *SNMP Add Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP V1 and SNMP V2c.

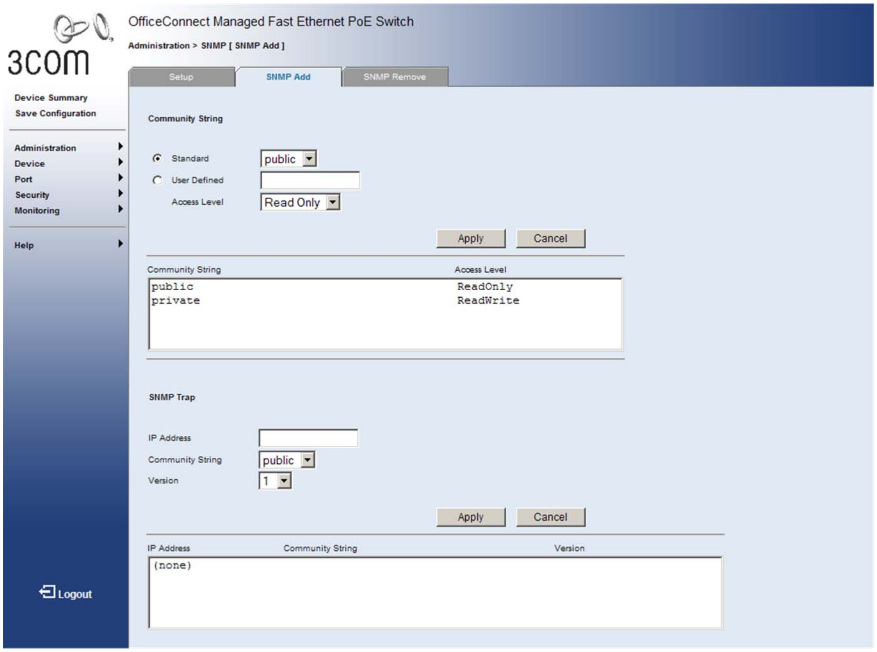
Filters that determine whether traps are sent to specific users, and the trap type sent can also be configured on the *SNMP Add Page*.

Monitor users have no access to this page.

To define SNMP communities:

1 Click **Administration > SNMP > SNMP Add**. The *SNMP Add Page* opens:

Figure 85 SNMP Add Page



Community String

● Standard public

○ User Defined

Access Level Read Only

Community String	Access Level
public	ReadOnly
private	ReadWrite

SNMP Trap

IP Address

Community String public

Version 1

IP Address	Community String	Version
(none)		

The *SNMP Add Page* contains the following fields:

Community String

- **Standard** — Selects pre-defined community strings. The possible field values are:
    - *public* — Displays the pre-defined public community string name. Fixed at read-only access.
    - *private* — Displays the pre-defined private community string name. Fixed at read/write access.
- **User Defined** — Defines a user-defined community string name. The maximum string length is 32 characters, all case sensitive. The maximum number of strings is 5.
- **Access Level** — Defines the access rights of the community. The possible field values are:
    - *Read Only* — Management access is restricted to read-only. Authorized management stations are only able to retrieve MIB objects.
    - *Read Write* — Management access is read/write. Authorized management stations are able to both retrieve and modify MIB objects.

SNMP Trap

- **IP Address** — Defines the IP address to which the traps are sent. A maximum of 5 recipient destination IP address entries can be defined
- **Community String** — Defines the community string of the trap manager. The maximum string length is 32 characters, all case sensitive.
- **Version** — Specifies the trap type. The possible field values are:
    - *1* — Indicates that SNMP Version 1 traps are sent.
    - *2c* — Indicates that SNMP Version 2c traps are sent.

2 Define the relevant fields.

3 Click Apply. The SNMP Communities and SNMP Traps are defined, and the device is updated.

Removing SNMP Communities or Traps

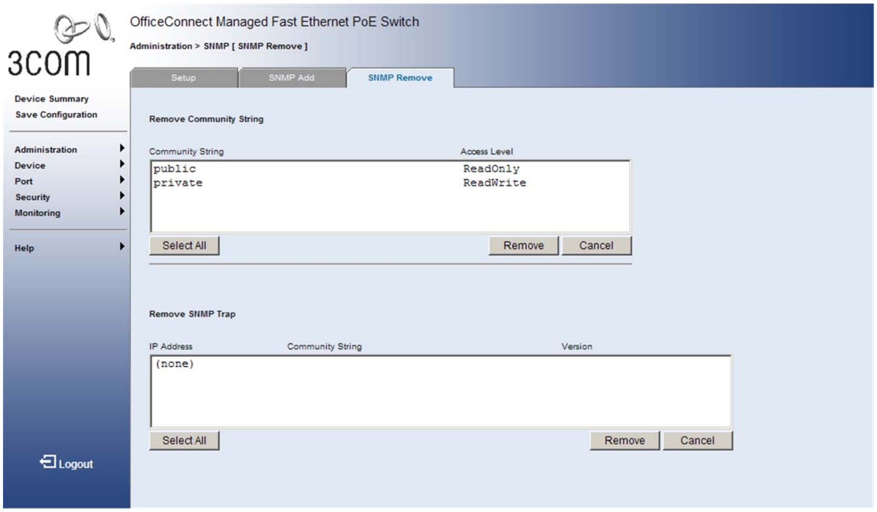
The *SNMP Remove Page* allows the system manager to remove SNMP Communities.

Monitor users have no access to this page.

To remove SNMP communities or traps:

1 Click **Administration > SNMP > SNMP Remove**. The *SNMP Remove Page* opens:

Figure 86 SNMP Remove Page



Remove Community String

Community String	Access Level
public	ReadOnly
private	ReadWrite

Remove SNMP Trap

IP Address	Community String	Version
(none)		

The *SNMP Remove Page* contains the following fields:

Remove Community String

- **Community String** — Displays the user-defined text string which authenticates management stations to the device.
- **Access Level** — Displays the access rights of the community. The possible field values are:
  - *Read Only* — Management access is restricted to read-only. Authorized management stations are only able to retrieve MIB objects.
  - *Read Write* — Management access is read/write. Authorized management stations are able to both retrieve and modify MIB objects.

Remove SNMP Trap

- **IP Address** — Displays the management station IP address for which the SNMP community is defined.
- **Community String** — Displays the user-defined text string which authenticates the management station to the device.
- **Version** — Displays the trap type. The possible field values are:
  - *v1* — Indicates that SNMP Version 1 traps are sent.
  - *v2c* — Indicates that SNMP Version 2 traps are sent.

2. For each SNMP Community or Trap to be removed, select the table entry.
3. Click Remove. The SNMP Communities and Traps are removed, and the device is updated.

13 CONFIGURING QUALITY OF SERVICE

Quality of Service (QoS) provides the ability to implement QoS and priority queuing within a network. For example, certain types of traffic that require minimal delay, such as Voice, Video, and real-time traffic can be assigned a high priority queue, while other traffic can be assigned a lower priority queue. The result is an improved traffic flow for traffic with high demand. QoS is defined by:

- **Classification** — Specifies which packet fields are matched to specific values. All packets matching the user-defined specifications are classified together.
- **Action** — Defines traffic management where packets to be forwarded are based on packet information, and packet field values such as *VLAN Priority Tag* (VPT) and *DiffServ Code Point* (DSCP).
- **VPT Classification Information** — *VLAN Priority Tags* (VPT) are used to classify packets by mapping packets to one of the egress queues. VPT to Queue assignments are user-definable. Packets arriving untagged are assigned a default VPT value, which is set on a per-port basis. The assigned VPT is used to map the packet to the egress queue.

This section contains information for configuring QoS, and includes the following topics:

- Viewing CoS Settings
- Defining CoS
- Defining the Queue Mode
- Viewing CoS to Queue Mapping
- Defining CoS to Queue Mapping
- Viewing DSCP to CoS Mapping
- Configuring DSCP to CoS Mapping
- Configuring Trust Settings
- Viewing Bandwidth Settings
- Defining Bandwidth Settings
- Configuring Voice VLAN

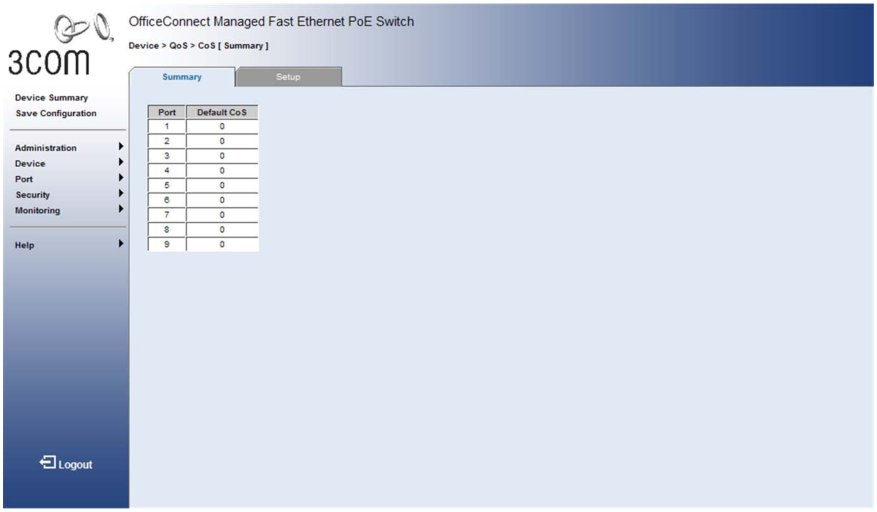
Viewing CoS Settings

The *CoS Summary Page* displays the CoS default settings assigned to each port.

To view CoS Settings:

1 Click **Device > QoS > CoS > Summary**. The *CoS Summary Page* opens:

Figure 87 CoS Summary Page



Port	Default CoS
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0

The *CoS Summary Page* contains the following fields:

- **Port** — Displays the port for which the CoS default value is defined.
- **Default CoS** — Displays the default CoS value for incoming packets for which a VLAN priority tag is not defined. The possible field values are *0-7*.

Defining CoS

The *CoS Setup Page* allows the network administrator to set the priority for incoming untagged frames.

The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

This switch provides four priority queues for each port. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

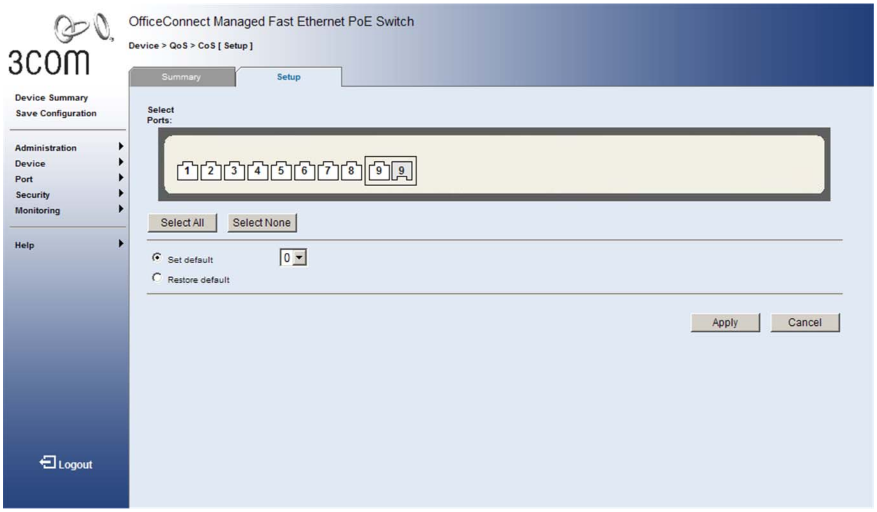
For tagged frames, the precedence for priority mapping is IP DSCP and then default port priority.

Monitor users have no access to this page.

To configure CoS Settings:

1 Click **Device > QoS > CoS> Setup**. The *CoS Setup Page* opens:

Figure 88 CoS Setup Page



● Set default 0

○ Restore default

The *CoS Setup Page* contains the following fields:

- **Select Ports** — Selects the ports to be configured.
- **Set default** — Sets the default user priority. The possible field values are *0-7*, where *0* is the lowest and *7* is the highest priority.
- **Restore Default** — Restores the device factory defaults for CoS values.

2 Define the fields.

3 Click Apply. CoS is configured on the device, and the device is updated.

Defining the Queue Mode

The *Queue Setup Page* is used to set the queue mode to strict priority or Weighted Round-Robin (WRR) for the CoS priority queues.

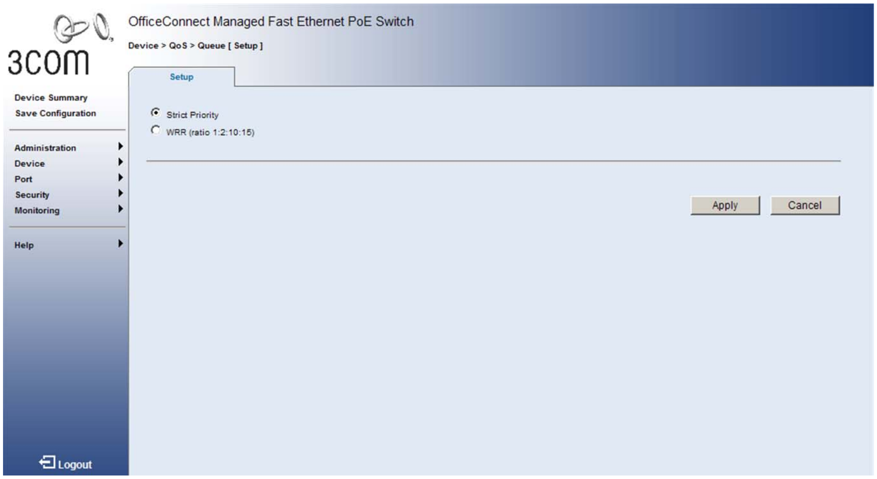
You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies the relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Monitor users have no access to this page.

To configure the queue mode:

1 Click **Device > QoS > Queue**. The *Queue Setup Page* opens:

Figure 89 Queue Setup Page



● Strict Priority
○ WRR (ratio 1:2:10:15)

The *Queue Setup Page* contains the following fields:

- **Strict Priority** — Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **WRR** — Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 10, 15 for queues 0 - 3 respectively.

2 Select the queue mode.

3 Click Apply. The queue mode is configured on the device, and the device is updated.

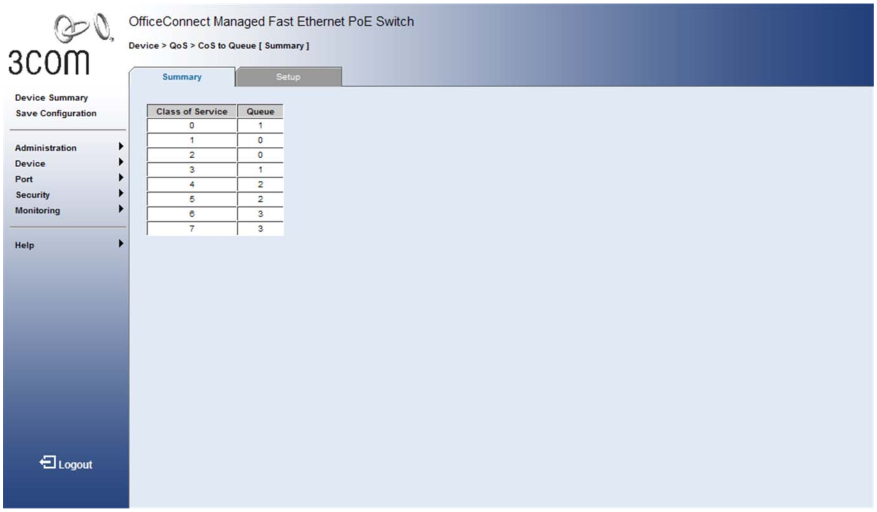
Viewing CoS to Queue Mapping

The *CoS to Queue Summary Page* contains a table that displays the CoS values mapped to four traffic queues. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard.

To view CoS Values to Queues:

1 Click **Device > QoS > CoS to Queue > Summary**. The *CoS to Queue Summary Page* opens:

Figure 90 CoS to Queue Summary Page



Class of Service	Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

The *CoS to Queue Summary Page* contains the following fields:

- **Class of Service** — Displays the CoS priority tag values, where *0* is the lowest and *7* is the highest.
- **Queue** — Indicates the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported.

Defining CoS to Queue Mapping

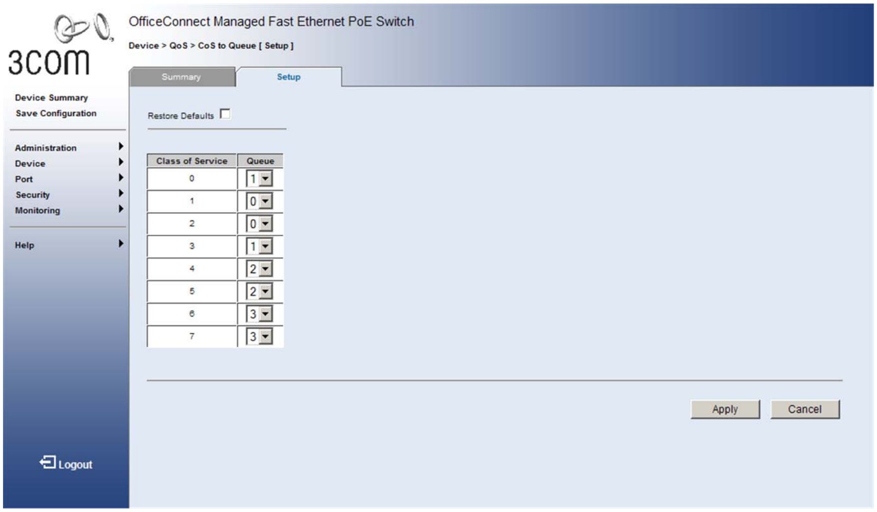
The *CoS to Queue Setup Page* contains fields for mapping CoS values to traffic queues. Four traffic priority queues are supported on the device, with 0 representing the lowest queue and 3 as the highest.

Monitor users have no access to this page.

To configure CoS values to queues:

1 Click **Device > QoS > CoS to Queue > Setup**. The *CoS to Queue Setup Page* opens:

Figure 91 CoS to Queue Setup Page



Restore Defaults □

Class of Service	Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

The *CoS to Queue Setup Page* contains the following fields:

- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.
- **Class of Service** — Specifies the CoS priority tag values, where *0* is the lowest and *7* is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped.

2 Define the queue number in the *Queue* field next to the required CoS value.

3 Click Apply. The CoS value is mapped to a queue, and the device is updated.

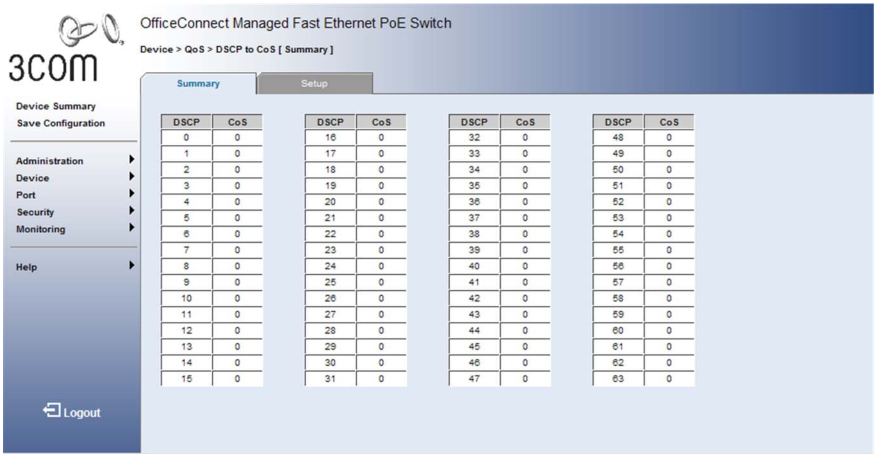
Viewing DSCP to CoS Mapping

The *DSCP to CoS Summary Page* displays the mapping of DSCP priority values to CoS values. DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four traffic queues.

To view the DSCP to CoS mapping:

1 Click **Device > QoS > DSCP to CoS > Summary**. The *DSCP to CoS Summary Page* opens:

Figure 92 DSCP to CoS Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > DSCP to CoS [Summary]

DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	0	16	0	32	0	48	0
1	0	17	0	33	0	49	0
2	0	18	0	34	0	50	0
3	0	19	0	35	0	51	0
4	0	20	0	36	0	52	0
5	0	21	0	37	0	53	0
6	0	22	0	38	0	54	0
7	0	23	0	39	0	55	0
8	0	24	0	40	0	56	0
9	0	25	0	41	0	57	0
10	0	26	0	42	0	58	0
11	0	27	0	43	0	59	0
12	0	28	0	44	0	60	0
13	0	29	0	45	0	61	0
14	0	30	0	46	0	62	0
15	0	31	0	47	0	63	0

The *DSCP to CoS Summary Page* contains the following fields:

- **DSCP** — Displays the incoming packet’s DSCP priority value.
- **CoS** — Displays the Class-of-Service value to which the corresponding DSCP priority value is mapped.

Configuring DSCP to CoS Mapping

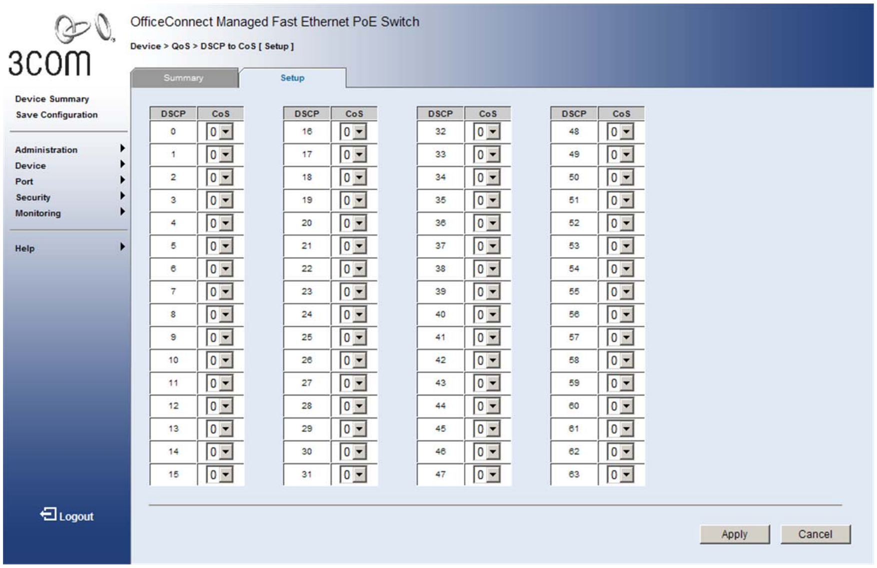
The *DSCP to CoS Setup Page* contains fields for mapping DSCP settings to traffic queues. DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four traffic queues.

Monitor users have no access to this page.

To map DSCP to CoS values:

1 Click **Device > QoS > DSCP to CoS > Setup**. The *DSCP to CoS Setup Page* opens:

Figure 93 DSCP to CoS Setup Page



DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	0	16	0	32	0	48	0
1	0	17	0	33	0	49	0
2	0	18	0	34	0	50	0
3	0	19	0	35	0	51	0
4	0	20	0	36	0	52	0
5	0	21	0	37	0	53	0
6	0	22	0	38	0	54	0
7	0	23	0	39	0	55	0
8	0	24	0	40	0	56	0
9	0	25	0	41	0	57	0
10	0	26	0	42	0	58	0
11	0	27	0	43	0	59	0
12	0	28	0	44	0	60	0
13	0	29	0	45	0	61	0
14	0	30	0	46	0	62	0
15	0	31	0	47	0	63	0

The *DSCP to CoS Setup Page* contains the following fields:

- **DSCP** — Displays the incoming packet's DSCP priority value.
- **CoS** — Specifies the Class-of-Service value to which the corresponding DSCP priority value is mapped.

2 Define the CoS value in the *CoS* field next to the required DSCP value.

3 Click Apply. The DSCP values are mapped to a CoS value, and the device is updated.

Configuring Trust Settings

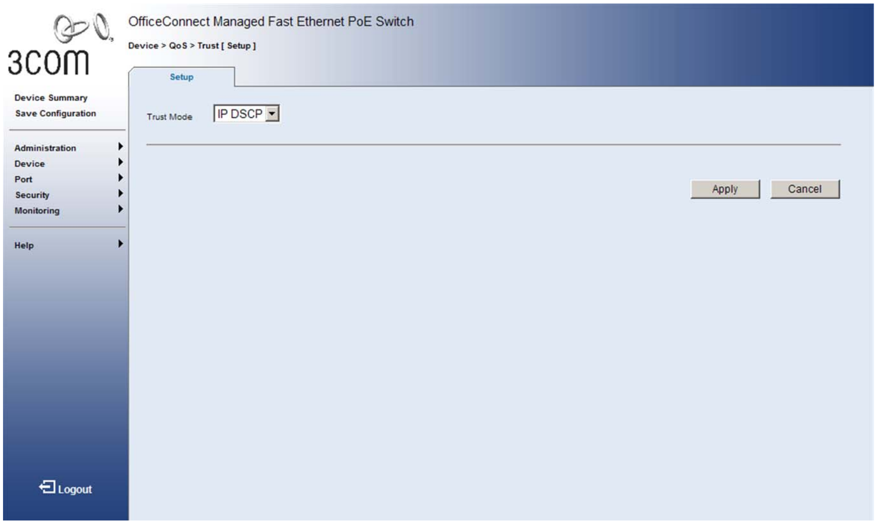
The *Trust Setup Page* is used to enable the processing of priority tags in ingress packets based on IP DSCP priority values or CoS values. Ingress packets are processed in the following manner:

- If the trust mode is set to IP DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- If the trust mode is set to IP DSCP, and a non-IP packet is received, the packet's CoS value is used for priority processing if the packet is tagged. For an untagged packet, the default port priority is used for priority processing.
- If the trust mode is set to CoS, and the ingress packet type is IPv4, then priority processing will be based on the CoS value in the ingress packet. For an untagged packet, the default port priority is used for priority processing.

To select the trust mode:

1 Click **Device > QoS > Trust > Setup**. The *Trust Setup Page* opens:

Figure 94 Trust Setup Page



Trust Mode: IP DSCP

The *Trust Setup Page* contains the following fields:

- **Trust Mode** — Specifies which packet fields to use for classifying packets entering the device. The possible Trust Mode field values are:
  - *CoS* — Classifies traffic based on the CoS tag value.
  - *DSCP* — Classifies traffic based on the IP DSCP tag value.

2 Define the trust mode.

3 Click Apply. The selected Trust mode is enabled on the device.

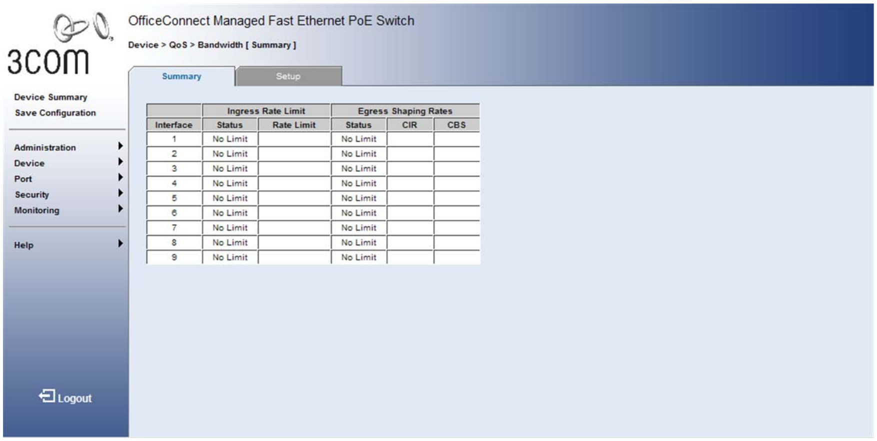
Viewing Bandwidth Settings

The *Bandwidth Summary Page* displays bandwidth settings for each interface.

To view Bandwidth Settings:

1 Click **Device > QoS > Bandwidth > Summary**. The *Bandwidth Summary Page* opens:

Figure 95 Bandwidth Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > Bandwidth [Summary]

	Ingress Rate Limit		Egress Shaping Rates		
Interface	Status	Rate Limit	Status	CIR	CBS
1	No Limit		No Limit		
2	No Limit		No Limit		
3	No Limit		No Limit		
4	No Limit		No Limit		
5	No Limit		No Limit		
6	No Limit		No Limit		
7	No Limit		No Limit		
8	No Limit		No Limit		
9	No Limit		No Limit		

The *Bandwidth Summary Page* contains the following fields:

- **Interface** — Displays the interface for which rate limit and shaping parameters are defined.

Ingress Rate Limit

- **Status** — Indicates the ingress rate limiting status on the interface. The possible field values are:
  - *Enabled* — Ingress rate limiting is enabled on the interface.
  - *No Limit* — Ingress rate limiting is disabled on the interface. This is the default.
- **Rate Limit** — Indicates the ingress traffic limit for the interface. The field options include 128, 1024, 5056, 10048, 50048, 100032 and 500032 kbits per second.

When using the command line interface, the field range is *64-100,000* kbits per second for Fast Ethernet ports, and *64-1,000,000* kbits per second for Gigabit Ethernet ports, at a resolution of 64 kbits per seconds.

Egress Shaping Rates

- **Status** — Indicates the egress traffic shaping status for the interface. The possible field values are:
  - *Enabled* — Egress traffic shaping is enabled for the interface.
  - *No Limit* — Egress traffic shaping is disabled for the interface. This is the default.
- **CIR** — Indicates the Committed Information Rate (CIR) for the interface. The field options include 128, 1024, 5056, 10048, 50048, 100032 and 500032 kbits per second.

  When using the command line interface, the field range is *64-100,000* kbits per second for Fast Ethernet ports, and *64-1,000,000* kbits per second for Gigabit Ethernet ports, at a resolution of 64 kbits per seconds.
- **CBS** — Indicates the Committed Burst Size (CBS) for the interface. The field options include 64, 128, 256, 512, 1024, 2048, and 4096.

Defining Bandwidth Settings

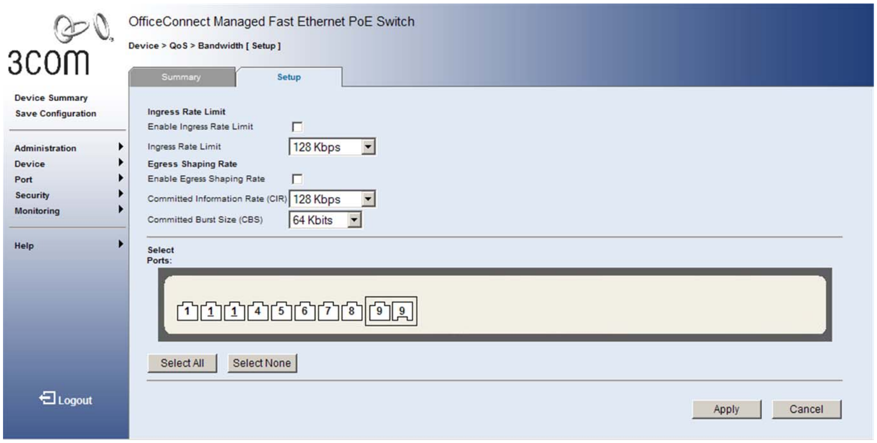
The *Bandwidth Setup Page* allows network managers to define the bandwidth settings for a specified interface. Interface shaping can be also be applied to the egress traffic on a specified interface.

Monitor users have no access to this page.

To configure Bandwidth Settings:

1 Click **Device > QoS > Bandwidth > Setup**. The *Bandwidth Setup Page* opens:

Figure 96 Bandwidth Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > Bandwidth [Setup]

Ingress Rate Limit

Enable Ingress Rate Limit □

Ingress Rate Limit: 128 Kbps

Egress Shaping Rate

Enable Egress Shaping Rate □

Committed Information Rate (CIR): 128 Kbps

Committed Burst Size (CBS): 64 Kbits

Select Ports:

The *Bandwidth Setup Page* contains the following fields:

Ingress Rate Limit

- **Enable Ingress Rate Limit** — Enables setting an Ingress Rate Limit.
- **Ingress Rate Limit** — Defines the ingress traffic limit for the port. The field options include 128, 1024, 5056, 10048, 50048, 100032 and 500032 kbits per second.

  When using the command line interface, the field range is *64-100,000* kbits per second for Fast Ethernet ports, and *64-1,000,000* kbits per second for Gigabit Ethernet ports at a resolution of 64 kbits per seconds.

Egress Shaping Rate

- **Enable Egress Shaping Rate** — Enables setting Egress Shaping Rates.
- **Committed Information Rate (CIR)** — Defines the CIR for the interface. The field options include 128, 1024, 5056, 10048, 50048, 100032 and 500032 kbits per second.

  When using the command line interface, the field range is *64-100,000* kbits per second for Fast Ethernet ports, and *64-1,000,000* kbits per second for Gigabit Ethernet ports at a resolution of 64 kbits per seconds.
- **Committed Burst Size (CBS)** — Defines the CBS for the interface. The field options include 64, 128, 512, 1024, 2048, and 4096 kbits.

  Rate limiting is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the CBS, and the average rate tokens at which are removed from the bucket is specified by the CIR.
- **Select ports** — Selects the ports to be configured.

2. Select the ports to be configured.
3. Define the fields.
4. Click Apply. The bandwidth is defined for the selected ports, and the device is updated.

Configuring Voice VLAN

The Voice VLAN allows network administrators to enhance VoIP service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Network Administrators can configure a VLAN on which voice IP traffic is forwarded. Non-VoIP traffic is dropped from the Voice VLAN in auto Voice VLAN secure mode. Voice VLAN also provides QoS to VoIP traffic, ensuring that the quality of voice does not deteriorate if IP traffic is received unevenly. The system supports one Voice VLAN.

There are two operational modes for IP Phones:

- IP phones are configured with VLAN-mode as enabled, ensuring that tagged packets are used for all communications.
- If the IP phone's VLAN-mode is disabled, the phone uses untagged packets. The phone uses untagged packets while retrieving the initial IP address through DHCP. The phone eventually uses the Voice VLAN and starts sending tagged packets.

This section contains the following topics:

- Viewing Voice VLAN
- Defining Voice VLAN
- Defining Voice VLAN Port Settings
- Viewing Voice VLAN Port Definitions
- Viewing the OUI Summaries
- Modifying OUI Definitions

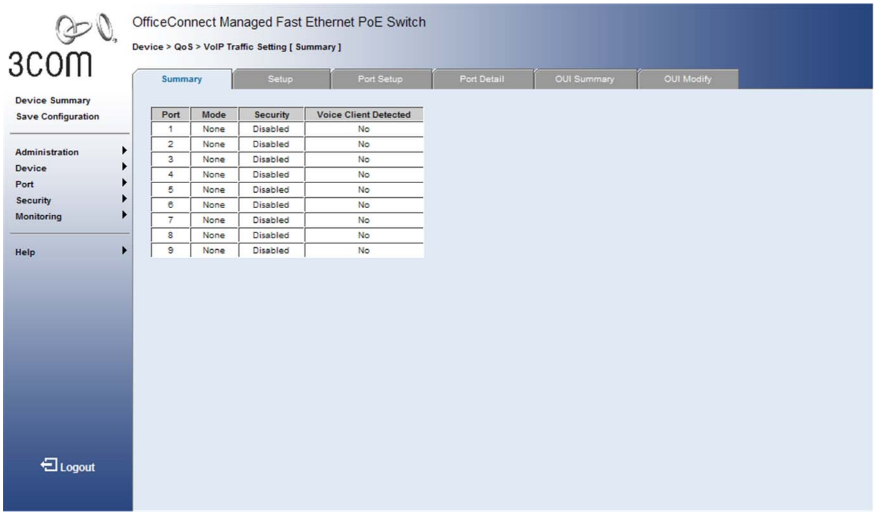
Viewing Voice VLAN

The *Voice VLAN Summary Page* contains information about the Voice VLAN currently enabled on the device, including the ports enabled and assigned to the Voice VLAN.

To view Voice VLAN Settings:

1 Click **Device > QoS > VoIP Traffic Setting > Summary**. The *Voice VLAN Summary Page* opens:

Figure 97 Voice VLAN Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > VoIP Traffic Setting [Summary]

Port	Mode	Security	Voice Client Detected
1	None	Disabled	No
2	None	Disabled	No
3	None	Disabled	No
4	None	Disabled	No
5	None	Disabled	No
6	None	Disabled	No
7	None	Disabled	No
8	None	Disabled	No
9	None	Disabled	No

The *Voice VLAN Summary Page* contains the following fields:

- **Port** — Displays a list of all switch ports.
- **Mode** — Specifies the Voice VLAN mode. The possible field values are:
  - *None* — Indicates that the selected port will not be added to the Voice VLAN.
  - *Manual* — Indicates that the selected port has been manually added to the Voice VLAN.
  - *Auto* — Indicates that if traffic with an IP Phone MAC address is transmitted on the port, the port will be added to the Voice VLAN.

- **Security** — Indicates if port security is enabled on the Voice VLAN. Port security ensures that packets arriving with an unrecognized MAC address are dropped.
  - *Enabled* — Enables port security on the Voice VLAN.
  - *Disabled* — Disables port security on the Voice VLAN. This is the default value.
- **Voice Client Detected** — Indicates if a voice client has been detected on the corresponding port.

Defining Voice VLAN

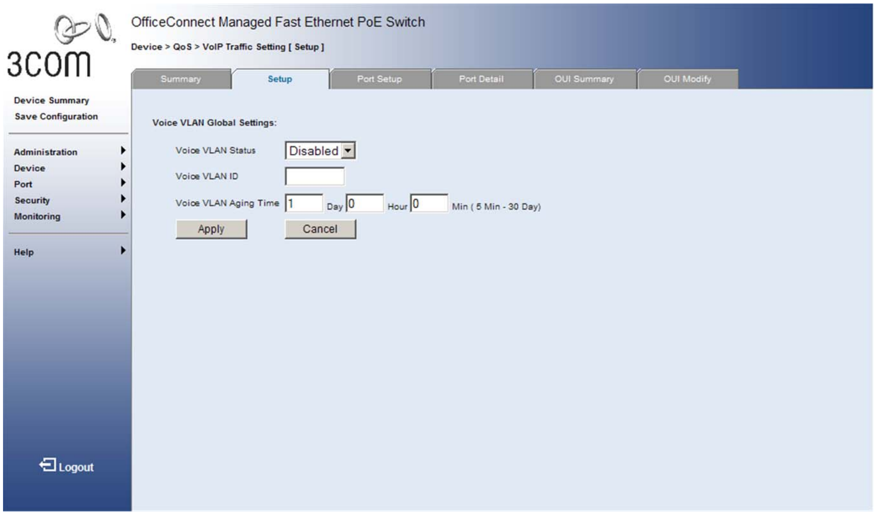
The *Voice VLAN Setup Page* provides information for enabling and defining Voice VLAN globally on the device.

Monitor users have no access to this page.

To configure Voice VLAN Settings:

1 Click **Device > QoS > VoIP Traffic Setting > Setup**. The *Voice VLAN Setup Page* opens:

Figure 98 Voice VLAN Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > VoIP Traffic Setting [Setup]

Voice VLAN Global Settings:

Voice VLAN Status: Disabled

Voice VLAN ID:

Voice VLAN Aging Time: 1 Day 0 Hour 0 Min (5 Min - 30 Day)

The *Voice VLAN Setup Page* contains the following fields:

- **Voice VLAN Status** — Enables or disables the Voice VLAN on the device. Remember to create a VLAN for voice traffic before enabling the Voice VLAN. The possible field values are:
  - *Enabled* — Enables Voice VLAN on the device.

  - *Disabled* — Disables Voice VLAN on the device. This is the default value.

- **Voice VLAN ID** — Defines the Voice VLAN ID number.
  (Range: 1-4094)

  Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.

  The Voice VLAN ID cannot be modified when auto-detection status is enabled for any port within the VLAN (see “Defining Voice VLAN Port Settings” on page 186).

- **Voice VLAN Aging Time** — Defines the amount of time after the last IP phone's OUI is aged out for a specific port. The Voice VLAN aging time starts after the MAC Address is aged out from the Dynamic MAC Address table. The port will age out after the bridge and voice aging times. The default bridge aging time is *300* seconds. The default voice aging time is *1* day. The possible fields are:

  - *Day* — The field range is *0-30*.
  - *Hour* — The field range is *0-23*.
  - *Minute* — The field range is *0-59*.

2 Select *Enabled* in the *Voice VLAN Status* field.

3 Define the *Voice VLAN ID* and *Voice VLAN Aging Time* fields.

4 Click Apply. The Voice VLAN is defined, and the device is updated.

Defining Voice VLAN Port Settings

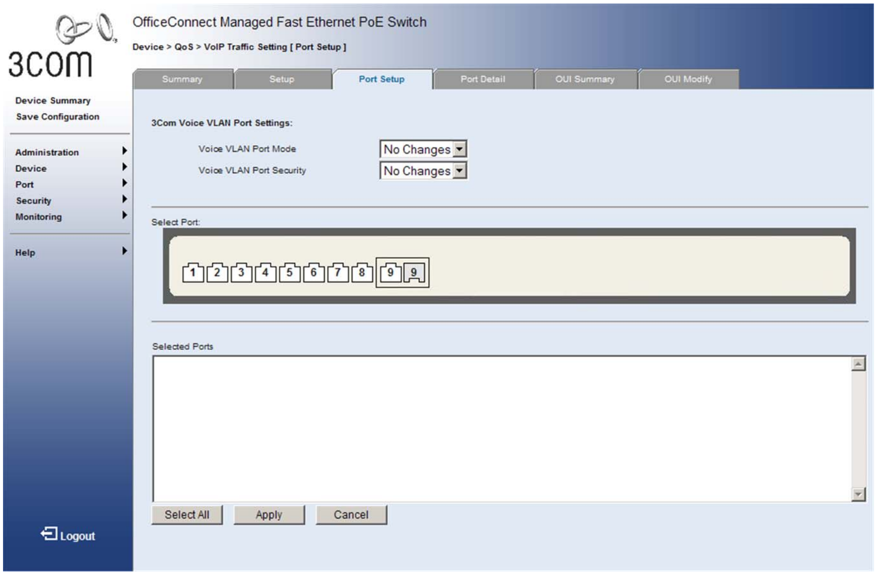
The *Voice VLAN Port Setup Page* contains information for defining Voice VLAN port settings.

Monitor users have no access to this page.

To configure Voice VLAN port settings:

1 Click **Device > QoS > VoIP Traffic Setting > Port Setup**. The *Voice VLAN Port Setup Page* opens:

Figure 99 Voice VLAN Port Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > QoS > VoIP Traffic Setting [Port Setup]

3Com Voice VLAN Port Settings:

Voice VLAN Port Mode: No Changes

Voice VLAN Port Security: No Changes

Select Port:

Selected Ports

The *Voice VLAN Port Setup Page* contains the following fields:

- **Voice VLAN Port Mode** — Specifies the Voice VLAN mode. The possible field values are:
  - *Auto* — Indicates that if traffic with an IP Phone MAC Address is transmitted on the port, the port joins the Voice VLAN. The port is aged out of the voice VLAN if the last IP phone’s MAC address (with a recognized OUI prefix) is aged out and the defined voice VLAN aging time is then exceeded. If the MAC Address of the IP phone’s OUI was added manually to a port in the Voice VLAN, you cannot add it to the Voice VLAN in Auto mode.
  - *Manual* — Adds a selected port to the Voice VLAN.
  - *None* — Indicates that the selected port will not be added to the Voice VLAN.

    - *No Changes* — Maintains the current Voice VLAN port settings. This is the default value.

  - **Voice VLAN Port Security** — Specifies if port security is enabled on the Voice VLAN. Port security ensures that packets arriving with an unrecognized MAC address are dropped.
    - *Enabled* — Enables port security on the Voice VLAN.
    - *Disabled* — Disables port security on the Voice VLAN. This is the default value.
    - *No Changes* — Maintains the current Voice VLAN port security settings.
  - **Select Port** — Enables selecting specific ports to which the Voice VLAN settings are applied. The ports are color-coded as follows:
    - *Blue* — Indicates the port is selected, and Voice VLAN settings are applied to the port.
    - *White* — Indicates the port is not selected, and the Voice VLAN settings are not applied to the port. This is the default value.
    - *Grey* — Indicates that the interface cannot be added to the Voice VLAN.
  - **Selected Ports** — Lists the ports on which the Voice VLAN settings are applied.

2 Select a port to configure. The port is highlighted blue.

3 Define the *Voice VLAN Port Mode* and *Voice VLAN Security* fields.

4 Click Apply. The Voice VLAN port settings are defined, and the device is updated.

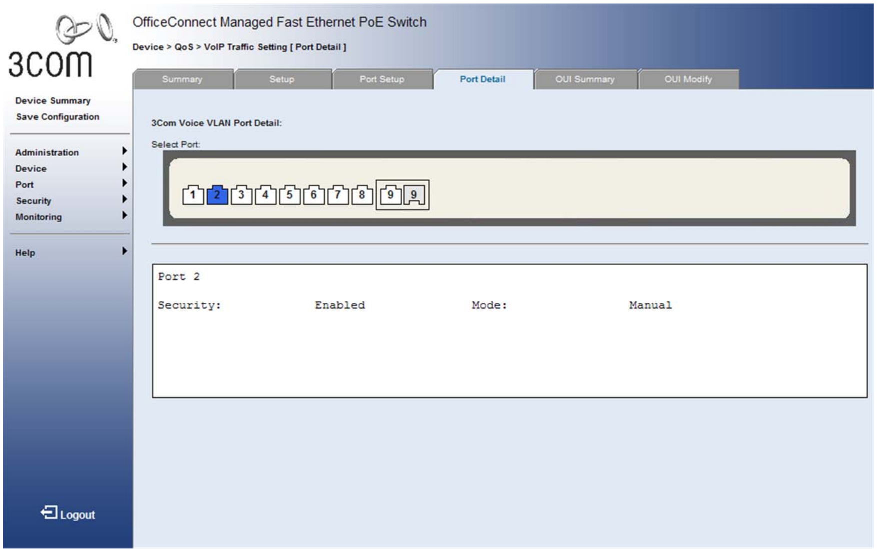
Viewing Voice VLAN Port Definitions

The *Voice VLAN Port Details Page* displays the Voice VLAN port settings for specific ports.

To view Voice VLAN Port Detail Settings:

1 Click **Device > QoS > VoIP Traffic Setting > Port Detail**. The *Voice VLAN Port Details Page* opens:

Figure 100 Voice VLAN Port Details Page



```
Port 2

Security:          Enabled          Mode:          Manual
```

The *Voice VLAN Port Details Page* contains the following fields:

- **Select Port** — Selects specific ports to display their Voice VLAN port definitions. The ports are color-coded as follows:
  - *Blue* — Indicates the port is selected, and its Voice VLAN settings are displayed in the text box below.
  - *White* — Indicates the port is not selected, and its Voice VLAN settings are not displayed. This is the default value.
  - *Grey* — Indicates that information cannot be displayed for this interface because it cannot be assigned to the Voice VLAN.

- **Port** — Displays the Voice VLAN port details for a selected port.
- **Security** — Indicates if port security is enabled on the Voice VLAN. Port Security ensures that packets arriving with an unrecognized MAC address are dropped.
    - *Enabled* — Enables port security on the Voice VLAN.
    - *Disabled* — Disables port security on the Voice VLAN. This is the default value.
- **Mode** — Displays the Voice VLAN mode. The possible field values are:
    - *None* — Indicates that the selected port will not be added to a Voice VLAN.
    - *Manual* — Indicates that the selected port has been manually added to the Voice VLAN.
    - *Auto* — Indicates that if traffic with an IP Phone MAC Address is transmitted on the port, the port will join the Voice VLAN. The port is aged out of the voice VLAN if the IP phone's MAC address (with a recognized OUI prefix) is aged out and the defined voice VLAN aging time is then exceeded.

2 Select a port to view its settings. The port is highlighted blue, and the Voice VLAN port settings are displayed in the text box.

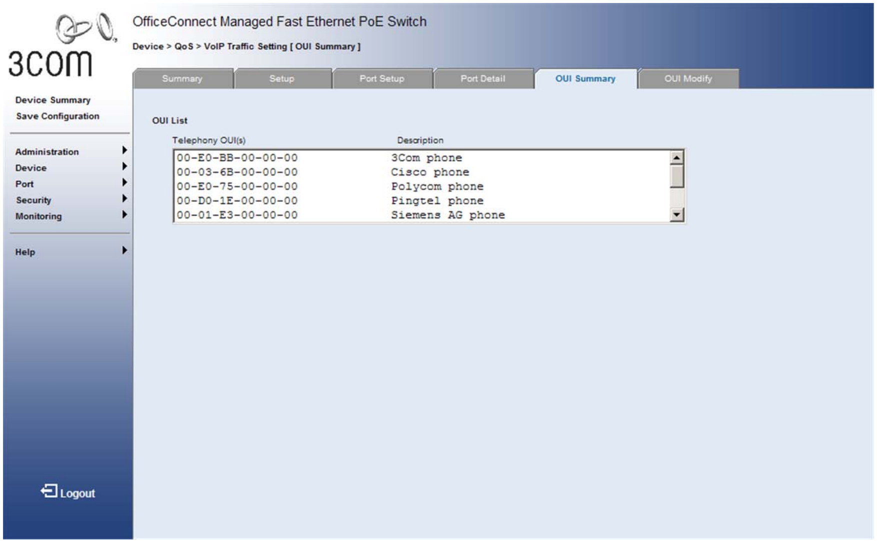
Viewing the OUI Summaries

The *Voice VLAN OUI Summary Page* lists the *Organizationally Unique Identifiers* (OUIs) associated with the Voice VLAN. The first three bytes of the MAC Address contain a manufacturer identifier. While the last three bytes contain a unique station ID. Using the OUI, network managers can add specific manufacturer's MAC addresses to the OUI table. Once the OUIs are added, all traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI, is forwarded on the voice VLAN.

To view Voice VLAN OUI Settings:

1 Click **Device > QoS > VoIP Traffic Setting > OUI Summary**. The *Voice VLAN OUI Summary Page* opens:

Figure 101 Voice VLAN OUI Summary Page



OUI List

Telephony OUI(s)	Description
00-E0-BB-00-00-00	3Com phone
00-03-6B-00-00-00	Cisco phone
00-E0-75-00-00-00	Polycom phone
00-D0-1E-00-00-00	Pingtel phone
00-01-E3-00-00-00	Siemens AG phone

The *Voice VLAN OUI Summary Page* contains the following fields:

OUI List

- **Telephony OUI(s)** — Lists the OUIs currently enabled on the Voice VLAN. The following OUIs are enabled by default.
  - *00:E0:BB* — Assigned to 3Com IP Phones.
  - *00:03:6B* — Assigned to Cisco IP Phones.
  - *00:E0:75* — Assigned to Polycom IP Phones.
  - *00:D0:1E* — Assigned to Pingtel IP Phones.
  - *00:01:E3* — Assigned to Siemens AG IP Phones.
  - *00:60:B9* — Assigned to Philips/NEC IP Phones.

  - *00:0F:E2* — Assigned to H3C Aolynk IP Phones.
  - *00:40:8C* — Assigned to Axis IP Cameras.
- **Description** — Displays the OUI description (up to 32 characters).

Modifying OUI Definitions

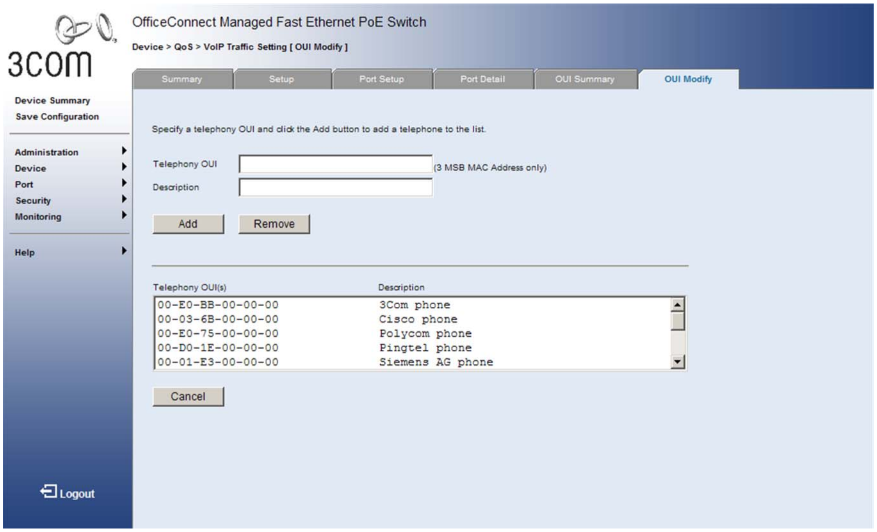
The *Voice VLAN OUI Modify Page* allows network administrators to add new OUIs or to remove previously defined OUIs from the Voice VLAN. The OUI is the first half (three most significant bytes) of the MAC address and is manufacturer specific, while the last three bytes contain a unique station ID. The packet priority derives from the source/destination MAC prefix. The packet gets higher priority when there is a match with the OUI list. Using the OUI, network managers can add a specific manufacturer's MAC addresses to the OUI table. Once the OUIs are added, all traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI, is forwarded on the voice VLAN.

Monitor users have no access to this page.

To modify Voice VLAN OUI Settings:

1 Click **Device > QoS > VoIP Traffic Setting > OUI Modify**. The *Voice VLAN OUI Modify Page* opens:

Figure 102 Voice VLAN OUI Modify Page



Specify a telephony OUI and click the Add button to add a telephone to the list.

Telephony OUI (3 MSB MAC Address only)

Description

Telephony OUI(s)	Description
00-E0-BB-00-00-00	3Com phone
00-03-6B-00-00-00	Cisco phone
00-E0-75-00-00-00	Polycom phone
00-D0-1E-00-00-00	Pingtel phone
00-01-E3-00-00-00	Siemens AG phone

The *Voice VLAN OUI Modify Page* contains the following fields:

- **Telephony OUI** — Defines a new or existing OUI on the Voice VLAN. The field contains the 3 most significant bytes of the MAC address.

- **Description** — Enters a user-defined OUI description. The field may contain up to 32 characters.
- **Add** — Allows you to add a new OUI.
- **Remove** — Allows you to delete an existing OUI.

2 Enter an OUI in the *Telephony OUI* field.

3 Enter an OUI description in the *Description* field.

4 Click Add to define a new OUI, or click Remove to delete an existing OUI. The Voice VLAN table is modified, and the device is updated.

14 MANAGING SYSTEM FILES

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or by downloading the configuration file via TFTP or HTTP.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, commands stored in the Running Configuration file and not yet saved to the Startup file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands already stored in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file by clicking on the *Save Configuration* button. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Image files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and to ensure that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

Backup and restore of the configuration files are always done from and to the Startup Configuration file.

This section contains information for defining File maintenance and includes both configuration file management as well as device access.

This section contains the following topics:

- Backing Up System Files
- Restoring Files
- Restoring the Software Image

Backing Up System Files

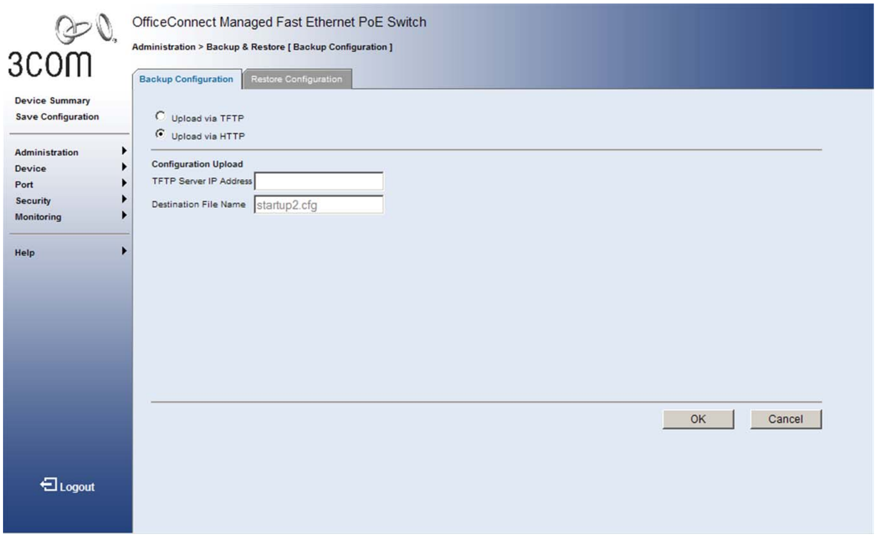
The *Backup Page* permits network managers to backup the system configuration to a TFTP or HTTP server.

Monitor users have no access to this page.

To backup System files:

1 Click **Administration > Backup & Restore > Backup**. The *Backup Page* opens:

Figure 103 Backup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Administration > Backup & Restore [Backup Configuration]

○ Upload via TFTP
● Upload via HTTP

Configuration Upload

TFTP Server IP Address

Destination File Name startup2.cfg

The *Backup Page* contains the following fields:

- **Upload via TFTP** — Enables initiating an upload to a TFTP server.
- **Upload via HTTP** — Enables initiating an upload to an HTTP server or HTTPS server.

Configuration Upload

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the configuration file is uploaded.
- **Destination File Name** — Specifies the destination file to which the configuration file is uploaded.

2 Define the relevant fields.

3 Click Apply. The backup file is defined, and the device is updated.

Restoring Files

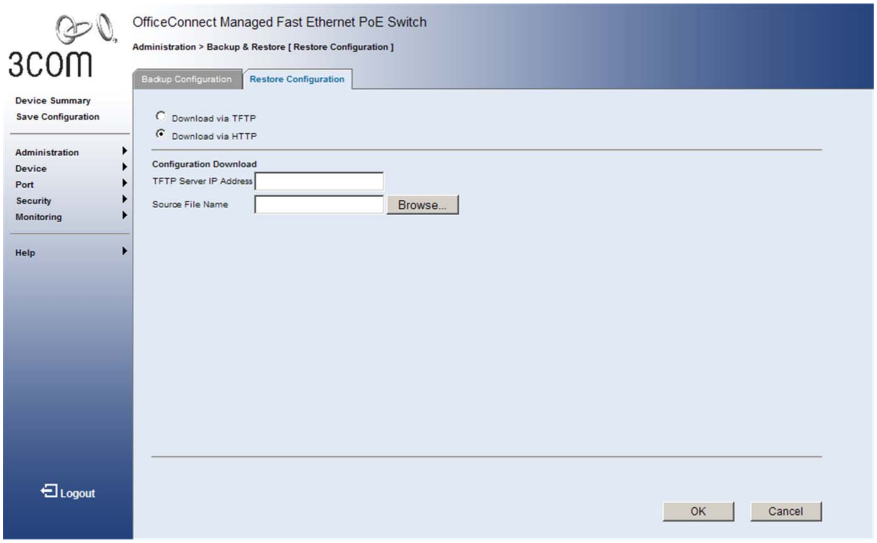
The *Restore Page* restores files from a TFTP or HTTP server.

Monitor users have no access to this page.

To restore System files:

1 Click **Administration > Backup & Restore > Restore**. The *Restore Page* opens:

Figure 104 Restore Page



OfficeConnect Managed Fast Ethernet PoE Switch

Administration > Backup & Restore [Restore Configuration]

○ Download via TFTP
● Download via HTTP

Configuration Download

TFTP Server IP Address

Source File Name

The *Restore Page* contains the following fields:

- **Download via TFTP** — Enables initiating a download from a TFTP server.
- **Download via HTTP** — Enables initiating a download from an HTTP server or HTTPS server.

Configuration Download

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which the configuration file is downloaded.
- **Source File Name** — Specifies the source file from which the configuration file is downloaded.

2 Define the relevant fields.

3 Click Apply. The restore file is defined, and the device is updated.

Restoring the Software Image

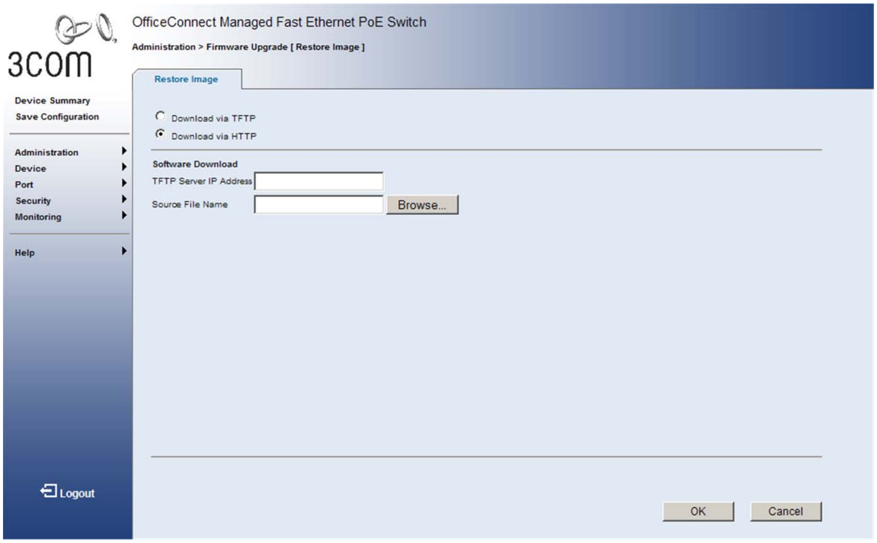
The *Restore Image Page* permits network managers to retrieve the device software.

Monitor users have no access to this page

To download the software image:

1 Click **Administration > Firmware Upgrade > Restore Image**. The *Restore Image Page* opens:

Figure 105 Restore Image Page



OfficeConnect Managed Fast Ethernet PoE Switch

Administration > Firmware Upgrade [Restore Image]

Restore Image

○ Download via TFTP
● Download via HTTP

Software Download

TFTP Server IP Address

Source File Name

The *Restore Image Page* contains the following fields:

- **Download via TFTP** — Enables initiating a download via a TFTP server.
- **Download via HTTP** — Enables initiating a download via an HTTP server or HTTPS server.

Software Download

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which the image file is downloaded.
- **Source File Name** — Specifies the image files to be downloaded.

2 Define the relevant fields.

3 Click Apply. The files are downloaded, and the device is updated.

15 MANAGING POWER OVER ETHERNET DEVICES

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources. Power over Ethernet can be used with:

- IP Phones
- Wireless Access Points
- IP Gateways
- PDAs
- Audio and video remote monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports.

This section contains information for configuring PoE Settings, and includes the following topics:

- Viewing PoE Settings
- Defining PoE Settings

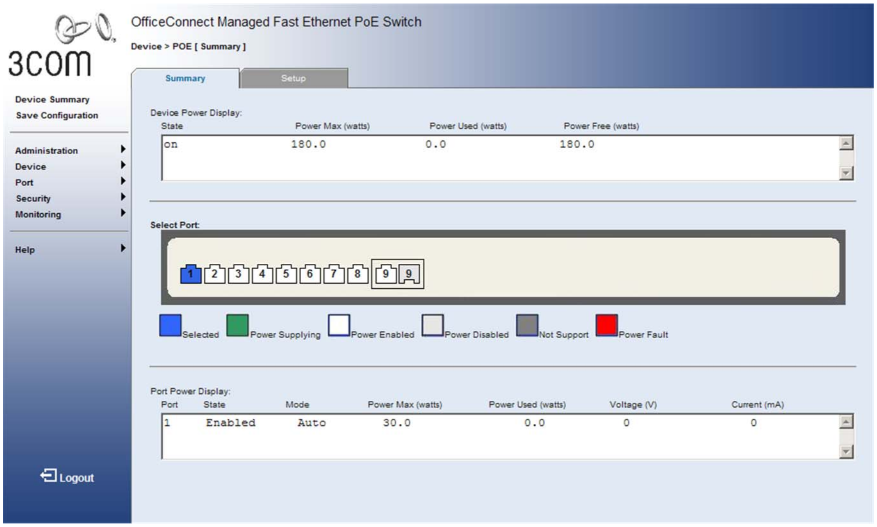
Viewing PoE Settings

The *Port PoE Summary Page* displays system PoE information on the device and attached ports, monitoring the current power usage and operational status.

To view PoE Settings:

1 Click **Port > PoE > Summary**. The *Port PoE Summary Page* opens:

Figure 106 Port PoE Summary Page



Device Power Display:

State	Power Max (watts)	Power Used (watts)	Power Free (watts)
on	180.0	0.0	180.0

Port Power Display:

Port	State	Mode	Power Max (watts)	Power Used (watts)	Voltage (V)	Current (mA)
1	Enabled	Auto	30.0	0.0	0	0

The *Port PoE Summary Page* displays the following information:

Device Power Display

- **State** — Indicates the in-line power source status. The possible field values are:
  - *on* — Indicates that the power supply unit is functioning.
  - *off* — Indicates that the power supply unit is not functioning.
- **Power Max** — Indicates the maximum amount of power the device can supply. The field value is displayed in Watts.
- **Power Used** — Indicates the actual amount of power currently used by the device. The field value is displayed in Watts.
- **Power Free** — Displays the amount of additional power currently available to the device. The field value is displayed in Watts.

- **Select Port** — Selects the ports to view PoE settings. The selected ports are color-coded as follows:
  - *Green* — Indicates the device is delivering power to the port.
  - *White* — Indicates the port is enabled for power delivery.
  - *Light Gray* — Indicates the port is disabled for power delivery.
  - *Dark Gray* — Indicates the port does not support PoE.
  - *Red* — Indicates a power fault.

Port Power Display

- **Port** — Indicates the port number.
- **State** — Indicates if the port is enabled to deliver power to powered devices. The possible field values are:
  - *Enabled* — Indicates the device is enabled to deliver power. This is the default.
  - *Disabled* — Indicates the device is not enabled to deliver power.
- **Mode** — Indicates the port power mode. The possible field values are:
  - *Auto* — Power is automatically allocated to the port, according to port number. Lower numbered ports are assigned a higher priority for power delivery. This is the default.
  - *Guarantee* — Power is guaranteed to the selected port, provided that the power is available. If the power demand from connected devices exceeds available power, this setting will override the priority assigned to higher numbered ports by the Auto mode.
- **Power Max** — Indicates the maximum amount of power available to the interface. The field value is displayed in Watts.
- **Power Used** — Indicates the actual amount of power currently used by the interface. The field value is displayed in Watts.
- **Voltage** — Indicates the voltage delivered to the interface. The field value is displayed in Volts.
- **Current** — Indicates the current delivered to the interface. The field value is displayed in milliAmperes.

Defining PoE Settings

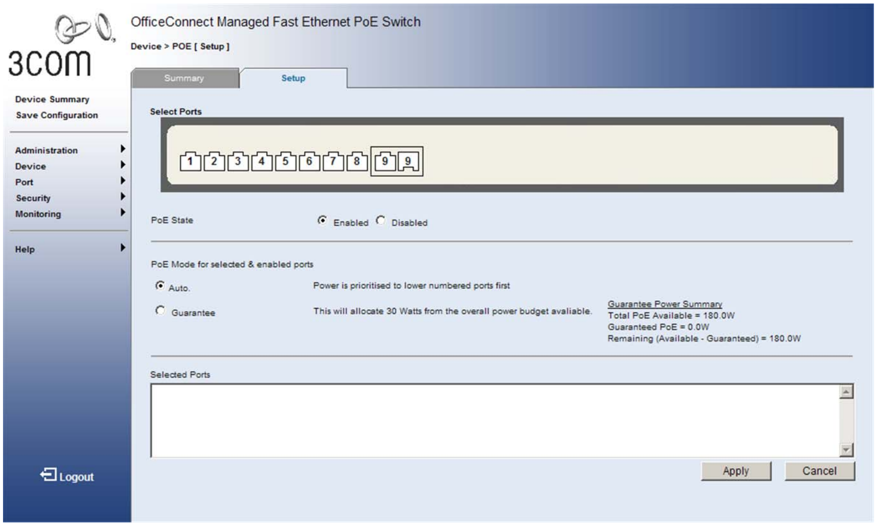
The *Port PoE Setup Page* allows users to configure ports for PoE.

Monitor users have no access to this page.

To configure Port PoE Settings:

1 Click **Port > PoE > Setup**. The *Port PoE Setup Page* opens:

Figure 107 Port PoE Setup Page



OfficeConnect Managed Fast Ethernet PoE Switch

Device > POE [Setup]

Select Ports

PoE State ● Enabled ○ Disabled

PoE Mode for selected & enabled ports

● Auto. Power is prioritised to lower numbered ports first

○ Guarantee This will allocate 30 Watts from the overall power budget avaliable.

Guarantee Power Summary
Total PoE Available = 180.0W
Guaranteed PoE = 0.0W
Remaining (Available - Guaranteed) = 180.0W

Selected Ports

The *Port PoE Setup Page* contains the following fields:

- **Select Ports** — Selects the ports to be configured.
- **PoE State** — Defines the port PoE state. The possible values are:
  - *Enabled* — Enables the port for PoE.
  - *Disabled* — Disables the port for PoE.
- **PoE Mode for selected & enabled ports** — Defines the PoE mode for the selected port. The possible values are:
  - *Auto* — Power is automatically allocated to the port, according to port number. Lower numbered ports are assigned a higher priority for power delivery.
  - *Guarantee* — Power is guaranteed to the selected port, provided that the power is available. This setting overrides the priority assigned to lower port numbers by the Auto mode.
- **Selected Ports** — Displays the ports selected to which the PoE configuration settings can be applied.

2 Define the fields.

3 Click Apply. The settings are applied to the selected ports, and the device is updated.

16 MANAGING SYSTEM LOGS

This section provides information for managing system logs. The system logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors and informational messages. Event messages have a unique format, according to the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent messages per each event.

The following table lists the log severity levels:

System Log Severity Levels

Severity	Level	Message
Emergency	0 (Highest)	The system is not functioning.
Alert	1	The system needs immediate attention.
Critical	2	The system is in a critical state.
Error	3	A system error has occurred.
Warning	4	A system warning has occurred.
Notice	5	The system is functioning properly, but a system notice has occurred.
Informational	6	Provides device information.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

This section includes the following topics:

- Viewing Logs
- Configuring Logging

Viewing Logs

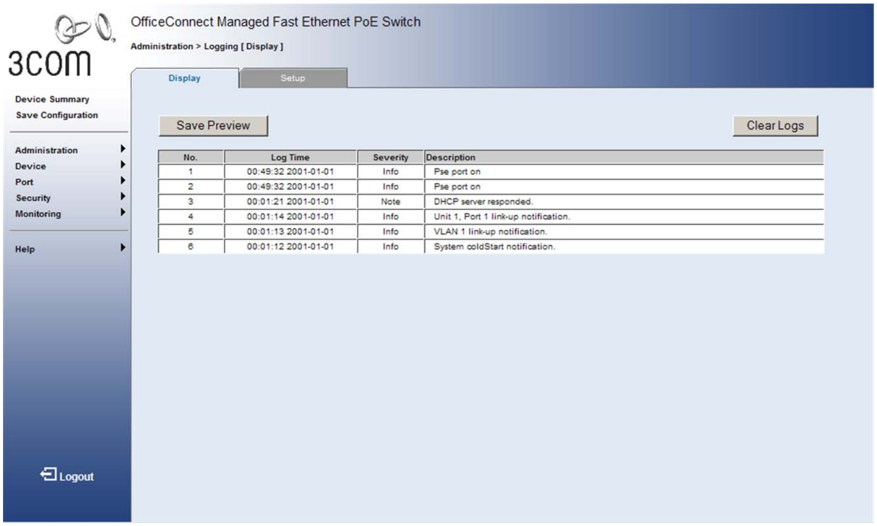
The *Logging Display Page* contains all system logs in chronological order that are saved in RAM (Cache).

Monitor users have no access to this feature.

To view Logging:

1 Click **Administration > Logging > Display**. The *Logging Display Page* opens:

Figure 108 Logging Display Page



No.	Log Time	Severity	Description
1	00:49:32 2001-01-01	Info	Pse port on
2	00:49:32 2001-01-01	Info	Pse port on
3	00:01:21 2001-01-01	Note	DHCP server responded.
4	00:01:14 2001-01-01	Info	Unit 1, Port 1 link-up notification.
5	00:01:13 2001-01-01	Info	VLAN 1 link-up notification.
6	00:01:12 2001-01-01	Info	System coldStart notification.

The *Logging Display Page* contains the following fields and buttons:

- **Save Preview** — Saves the displayed Log table to a web (HTML) page.
- **Clear Logs** — Deletes all logs from the Log table.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

2 Click Clear Logs . The selected logs are cleared, and the device is updated.

Configuring Logging

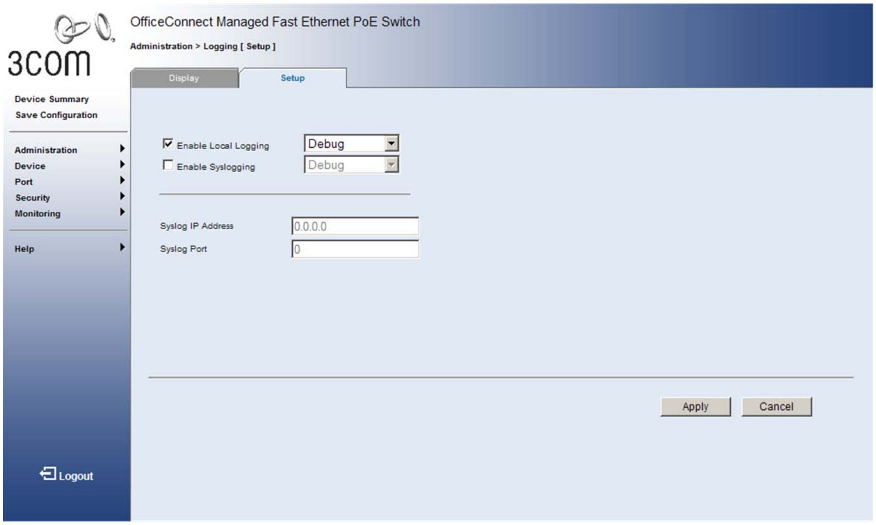
The *Logging Setup Page* contains fields for defining which events are recorded to which logs. It contains fields for enabling local logging or sending logs to Syslog servers.

Monitor users have no access to this feature.

To define Log Parameters:

1 Click **Administration > Logging > Setup**. *The Logging Setup Page* opens:

Figure 109 Logging Setup Page



☑ Enable Local Logging Debug
□ Enable Syslogging Debug

Syslog IP Address 0.0.0.0
Syslog Port 0

The *Logging Setup Page* contains the following fields:

- **Enable Local Logging** — Specifies if device logging to local Cache and Flash memory is enabled. Local logging is enabled by default.
- Severity level — Specifies the minimum severity level for which a message will be logged. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible field values are:
  - *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
  - *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.

  - *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
  - *Error* — A device error has occurred, for example, if a single port is offline.
  - *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
  - *Notice* — Provides device information.
  - *Info* — Provides device information.
  - *Debug* — Provides debugging messages.
- **Enable Syslogging** — Specifies if device logging to remote Syslogs servers is enabled.
- Severity level — Specifies the minimum severity level for which a message will be logged. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible field values are identical to those used for Local Logging.
- **Syslog IP Address** — Defines the IP Address of a syslog server to which syslog messages are sent.
- **Syslog Port** — Defines the UDP Port on the syslog server to which syslog messages are sent. The range for this field is *1-65535*, and the default is *514*.

2 Define the fields.

3 Click. Apply The log parameters are set, and the device is updated.

17 VIEWING STATISTICS

This section contains information for viewing port statistics, and contains the following topics:

- Viewing Port Statistics

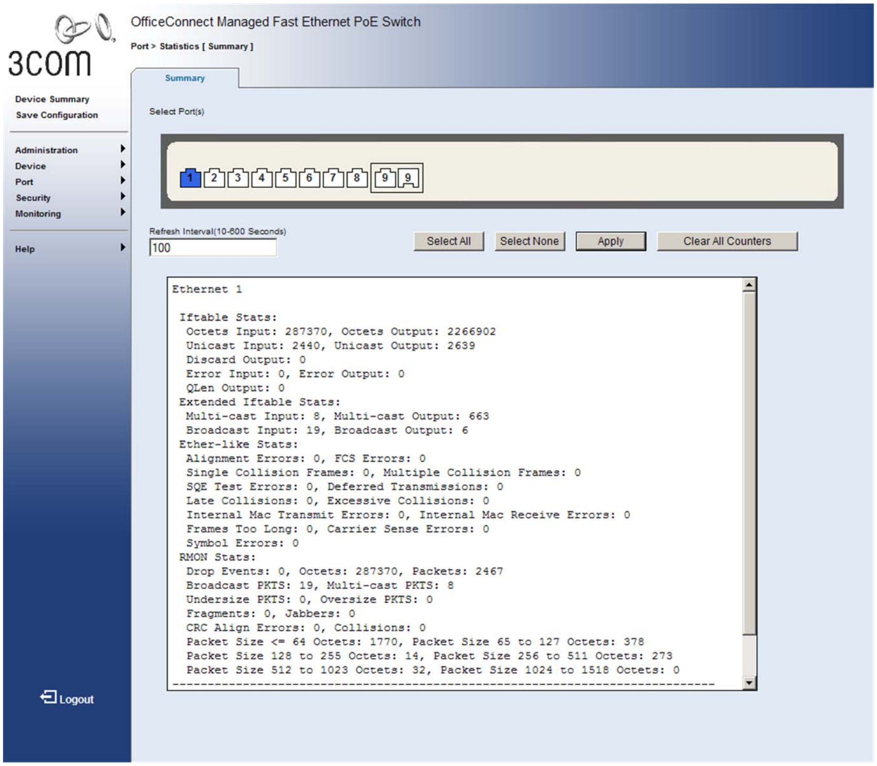
Viewing Port Statistics

The *Port Statistics Summary Page* contains fields for viewing information about device utilization and errors that occurred on the device.

To view port statistics:

1 Click **Ports > Statistics > Summary**. The *Port Statistics Summary Page* opens:

Figure 110 Port Statistics Summary Page



Refresh Interval(10-600 Seconds): 100

```
Ethernet 1

 Iftable Stats:
  Octets Input: 287370, Octets Output: 2266902
  Unicast Input: 2440, Unicast Output: 2639
  Discard Output: 0
  Error Input: 0, Error Output: 0
  QLen Output: 0
 Extended Iftable Stats:
  Multi-cast Input: 8, Multi-cast Output: 663
  Broadcast Input: 19, Broadcast Output: 6
 Ether-like Stats:
  Alignment Errors: 0, FCS Errors: 0
  Single Collision Frames: 0, Multiple Collision Frames: 0
  SQE Test Errors: 0, Deferred Transmissions: 0
  Late Collisions: 0, Excessive Collisions: 0
  Internal Mac Transmit Errors: 0, Internal Mac Receive Errors: 0
  Frames Too Long: 0, Carrier Sense Errors: 0
  Symbol Errors: 0
 RMON Stats:
  Drop Events: 0, Octets: 287370, Packets: 2467
  Broadcast PKTS: 19, Multi-cast PKTS: 8
  Undersize PKTS: 0, Oversize PKTS: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 Octets: 1770, Packet Size 65 to 127 Octets: 378
  Packet Size 128 to 255 Octets: 14, Packet Size 256 to 511 Octets: 273
  Packet Size 512 to 1023 Octets: 32, Packet Size 1024 to 1518 Octets: 0
------------------------------------------------------------------------------
```

The *Port Statistics Summary Page* contains the following fields:

- **Select Port** — Selects the specific port for which statistics are displayed.
- **Refresh Interval** — Defines the amount of time that passes before the interface statistics are refreshed. The field range is *10-600* seconds, and default is *10* seconds.

- Statistics — The Ethernet and RMON statistics displayed for the selected port are described in the following table.

Table 12 *Port Statistics Summary Page* - Field Description

Field	Description
Octets Input	The total number of octets received on the interface, including framing characters.
Octets Output	The total number of octets transmitted out of the interface, including framing characters.
Unicast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Unicast Output	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
Discard Output	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Error Input	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character- oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Error Output	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors
QLen Output	The length of the output packet queue (in packets).
Multicast Input	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.
Multicast Output	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.
Broadcast Input	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.

Table 12 *Port Statistics Summary Page* - Field Description (continued)

Field	Description
Broadcast Output	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.
Alignment Errors	The number of alignment errors (mis-synchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal Mac Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Internal Mac Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.

Table 12 *Port Statistics Summary Page* - Field Description (continued)

Field	Description
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII.
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Octets	The total number of octets received on the interface, including framing characters.
Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Broadcast PKTS	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.
Multicast PKTS	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.
Undersize PKTS	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.
Oversize PKTS	The total number of packets received that were longer than 1518 octets (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.
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.
CRC Align Errors	The number of CRC/alignment errors (FCS or alignment errors).

Table 12 *Port Statistics Summary Page* - Field Description (continued)

Field	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes Frames 65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 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).

2 Select a port.

3 Click Apply. The port statistics are displayed.

4 Click Clear All Counters. The port statistics counters are cleared and new statistics are displayed.

18 MANAGING DEVICE DIAGNOSTICS

This section contains information for viewing and configuring port and cable diagnostics, and includes the following topics:

- Configuring Port Mirroring
- Configuring Cable Diagnostics
- Pinging Another Device

Configuring Port Mirroring

You can mirror traffic from one or more source ports to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one or more ports to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables monitoring of switch performance.

Network administrators can configure port mirroring by selecting one or more ports from which to copy transmit or receive packets, and another port to which the packets are copied.

Port mirroring is not supported for trunk ports.

This section contains the following topics:

- Defining Port Mirroring
- Removing Port Mirroring

Defining Port Mirroring

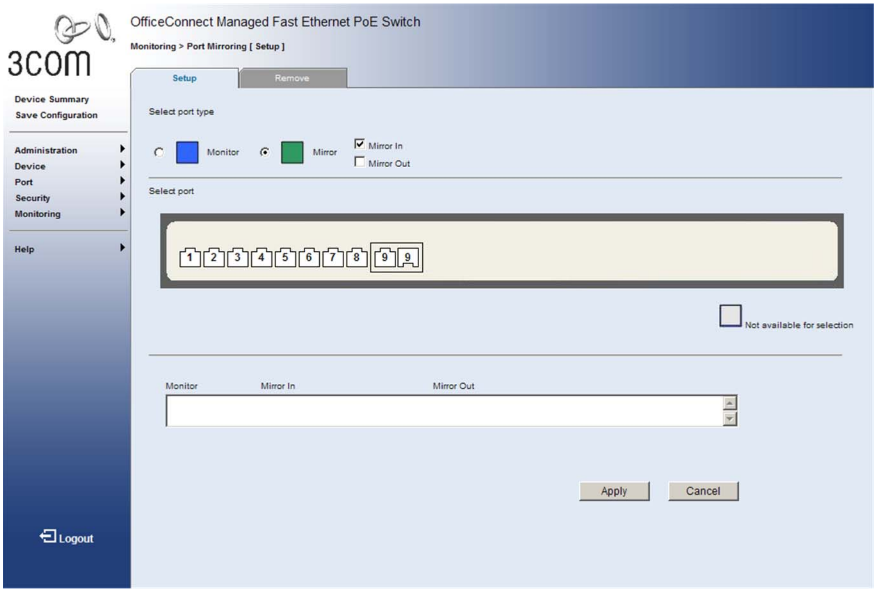
The *Port Mirroring Setup Page* contains parameters for configuring port mirroring.

Monitor users have no access to this page.

To enable port mirroring:

1 Click **Monitoring > Port Mirroring > Setup**. The *Port Mirroring Setup Page* opens:

Figure 111 Port Mirroring Setup Page



Select port type

○ 🟦 Monitor ● 🟩 Mirror ☑ Mirror In ☐ Mirror Out

The *Port Mirroring Setup Page* contains the following fields:

- **Select port type** — Defines the port that will be the monitor port (destination port) and the port that will be mirrored (source port). The possible values are:
  - *Monitor* — Defines the port as the monitor port, the destination port.
  - *Mirror* — Defines the port as a mirrored port (source port) to be monitored and indicates the traffic direction to be monitored. The possible values are:
    - *Mirror In* — Enables port mirroring on ingress traffic.
    - *Mirror Out* — Enables port mirroring on egress traffic.

- **Select port** — Selects the port for mirroring or monitoring. A port unavailable for mirroring is colored grey.
- Summary — Displays the current monitor and mirror port. The fields displayed are:
    - **Monitor** — Displays the monitor port.
    - **Mirror In** — Displays the ports monitored for ingress traffic.
    - **Mirror Out** — Displays the ports monitored for egress traffic.

2. Select a port type.
3. If the *Mirror* port type has been selected, select *Mirror In* and/or *Mirror Ou*t.
4. Select the *Monitor* port (destination port).
5. Click Apply. Port mirroring is enabled, and the device is updated.

Removing Port Mirroring

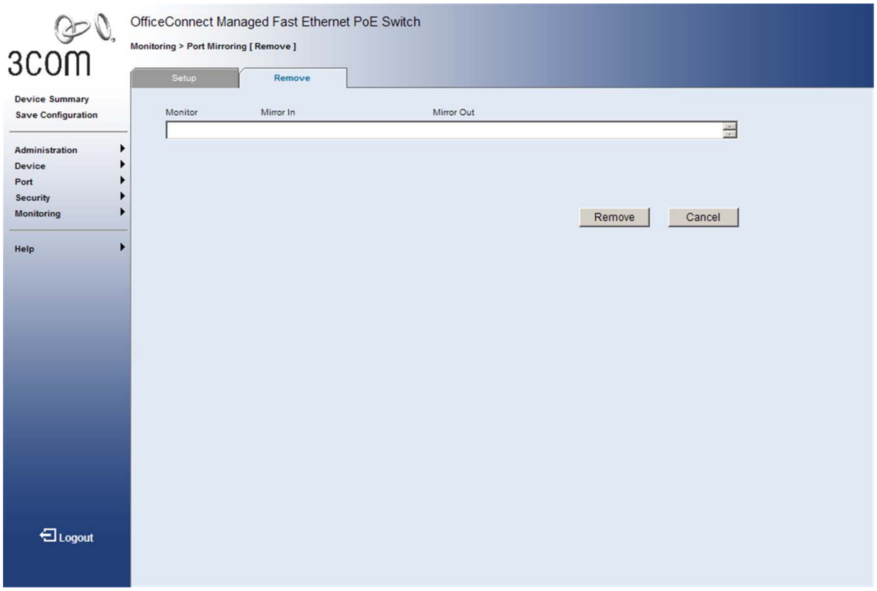
The *Port Mirroring Remove Page* permits the network manager to terminate port mirroring.

Monitor users have no access to this page.

To remove port mirroring:

1 Click **Monitoring > Port Mirroring > Remove**. The *Port Mirroring Remove Page* opens:

Figure 112 Port Mirroring Remove Page



The *Port Mirroring Remove Page* contains the following fields:

- **Monitor** — Displays the monitor port.
- **Mirror In** — Displays the ports monitored for ingress traffic.
- **Mirror Out** — Displays the ports monitored for egress traffic.

2 Select the ports to be removed.

3 Click Remove. Port mirroring is removed, and the device is updated.

Configuring Cable Diagnostics

Cable diagnostics perform basic connectivity tests on copper cables. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port.

This section contains the following topics:

- Viewing Cable Diagnostics
- Defining Cable Diagnostics

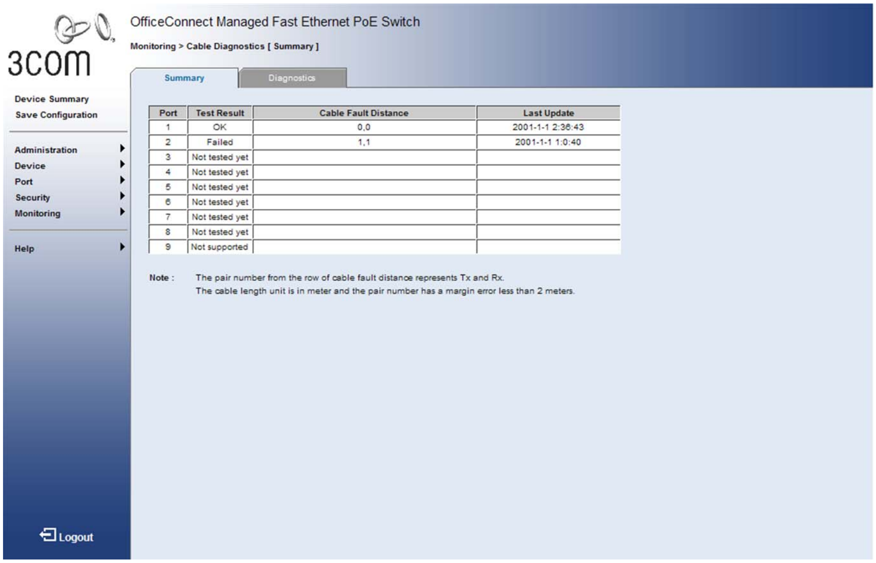
Viewing Cable Diagnostics

The *Cable Diagnostics Summary Page* contains fields for viewing tests on copper cables. Cable testing provides information about where errors occurred in the cable, and the last time a cable test was performed.

To view cables diagnostics:

1 Click **Monitoring > Cable Diagnostics > Summary**. The *Cable Diagnostics Summary Page* opens:

Figure 113 Cable Diagnostics Summary Page



OfficeConnect Managed Fast Ethernet PoE Switch

Monitoring > Cable Diagnostics [Summary]

Port	Test Result	Cable Fault Distance	Last Update
1	OK	0,0	2001-1-1 2:36:43
2	Failed	1,1	2001-1-1 1:0:40
3	Not tested yet		
4	Not tested yet		
5	Not tested yet		
6	Not tested yet		
7	Not tested yet		
8	Not tested yet		
9	Not supported		

Note : The pair number from the row of cable fault distance represents Tx and Rx.
The cable length unit is in meter and the pair number has a margin error less than 2 meters.

The *Cable Diagnostics Summary Page* contains the following fields:

- **Port** — Indicates the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
  - *OK* — Indicates that the cable passed the test.

  - *Failed* — Indicates that the cable failed the test. The test will fail if a cable is not connected to the port, the cable is connected on only one side, the cable is shorter than one meter, or a short has occurred in the cable.
- **Cable Fault Distance** — Indicates the distance in meters from the port where the cable error occurred. The number pair indicates the fault distance for transmit/receive signals.
- **Last Update** — Indicates the last time the port was tested.

Defining Cable Diagnostics

The *Diagnostics Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, and the last time a cable test was performed.

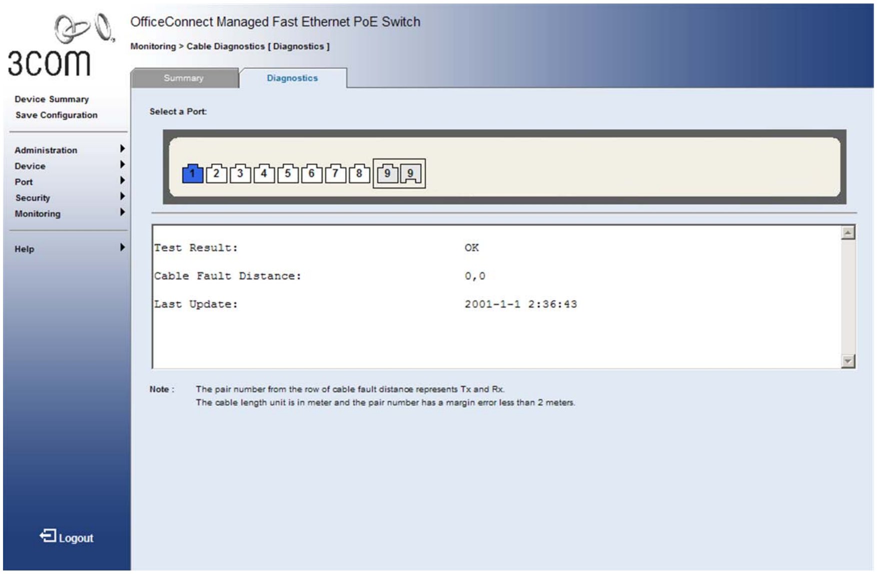
When performing cable tests consider the following:

- During the tests, ports are in the down state.
- The minimum cable length resolution is one meter, so if the cable is shorter than one meter the test will display "Failed."
- An open cable or a 2-pair copper cable will display a cable fault at a distance of 0 meters.
- The maximum cable length is 120 meters.

To test cables:

1 Click **Monitoring > Cable Diagnostics > Diagnostics**. The *Diagnostics Page* opens:

Figure 114 Diagnostics Page



OfficeConnect Managed Fast Ethernet PoE Switch

Monitoring > Cable Diagnostics [Diagnostics]

Select a Port:

```
Test Result:                                   OK
Cable Fault Distance:                          0,0
Last Update:                                   2001-1-1 2:36:43
```

Note : The pair number from the row of cable fault distance represents Tx and Rx.
The cable length unit is in meter and the pair number has a margin error less than 2 meters.

The *Diagnostics Page* contains the following fields:

- **Select a Port** — Selects the port to be tested.
- **Test Result** — Displays the cable test results. Possible values are:
  - *OK* — Indicates that the cable passed the test.
  - *Failed* — Indicates that the cable failed the test. The test will fail if a cable is not connected to the port, the cable is connected on only one side, the cable is shorter than one meter, or a short has occurred in the cable.
- **Cable Fault Distance** — Indicates the distance in meters from the port where the cable error occurred.

A Cable Fault Distance of 0M can result from a short (< 1 meter) cable, an open cable or a 2-pair copper cable.

- **Last Update** — Indicates the last time the port was tested.

2 Select a port to be tested. The port is tested, and the page is updated.

Pinging Another Device

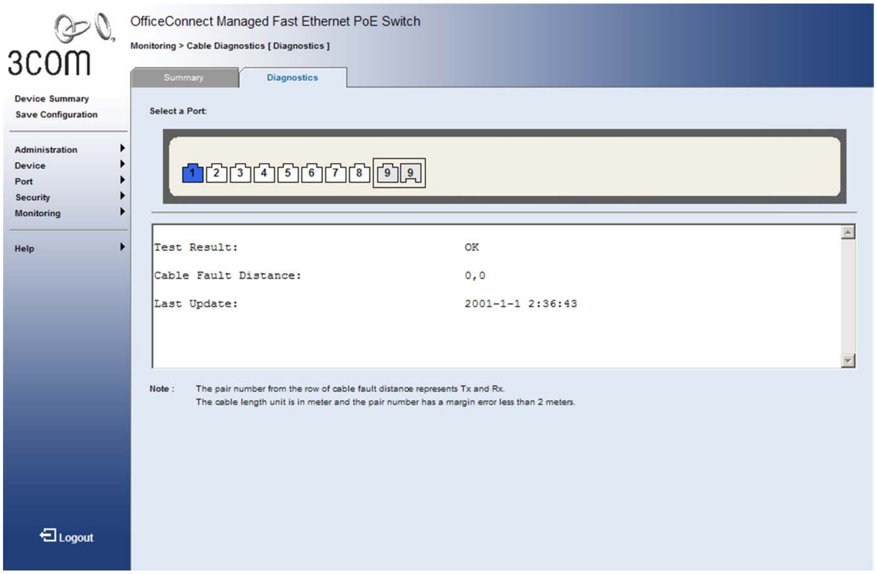
The *Ping Page* allows the network administrator to sends ICMP echo request packets to another node on the network.

Use the *Ping* command to see if another site on the network can be reached. The default number of packets to send is 5, and the default packet size is 32 bytes. Note that these parameters can be changed when using the command line interface to ping another device.

To send ping requests to another device:

1 Click **Monitoring > Ping**. The *Ping Page* opens:

Figure 115 Ping Page



```
Test Result:                    OK

Cable Fault Distance:           0,0

Last Update:                    2001-1-1 2:36:43
```

Note : The pair number from the row of cable fault distance represents Tx and Rx.
The cable length unit is in meter and the pair number has a margin error less than 2 meters.

The *Ping Page* contains the following fields:

- **IP Address** — IP address of the host.

2 Enter the IP address of the target device.

3 Click Start. The switch starts pinging the target device.

The following are some results of the *Ping* command:

- *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
- *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.

- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

Press <Esc> to stop pinging.

A 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

B DEVICE SPECIFICATIONS AND FEATURES

Related Standards

The 3Com® OfficeConnect Managed Fast Ethernet PoE 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), IEEE 802.3af (Power over Ethernet), IEEE 802.3at (Power over Ethernet Plus)
Safety	UL 60950-1, EN 60950-1, CSA 22.2 No. 60950-1, IEC 60950-1
EMC Emissions	EN55022 Class B, CISPR 22 Class B, FCC Part 15 Subpart B Class B, ICES-003 Class B, VCCI Class B, AS/NZS CISPR22 Class B
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	440 mm (17.3 in.)
Depth	265 mm (10.4 in.)
Height	43.6 mm (1.73 in.) or 1U.
Weight	2.04 kg (4.50 lb)
Mounting	Standalone mounting

Electrical

Line Frequency	50/60 Hz
Input Voltage	100–240 Vac (auto range)
Current Rating	2.0 Amp (Max)
Maximum Power Consumption	200.3 BTU/hr (88 Watts)
Max Heat Dissipation	200.3 BTU/hr

Switch Features

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

Table 13 Features of the OfficeConnect Managed Fast Ethernet PoE 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.
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.
Command Line Interface	The Command Line Interface (CLI) is an interface using a serial connection that allows the switch to be configured.

Table 13 Features of the OfficeConnect Managed Fast Ethernet PoE Switch (continued)

Feature	Description
Configuration File Management	The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration settings. 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.
Edge Port	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 Edge Port 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.

Table 13 Features of the OfficeConnect Managed Fast Ethernet PoE Switch (continued)

Feature	Description
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 *s*tandard 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 33.
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

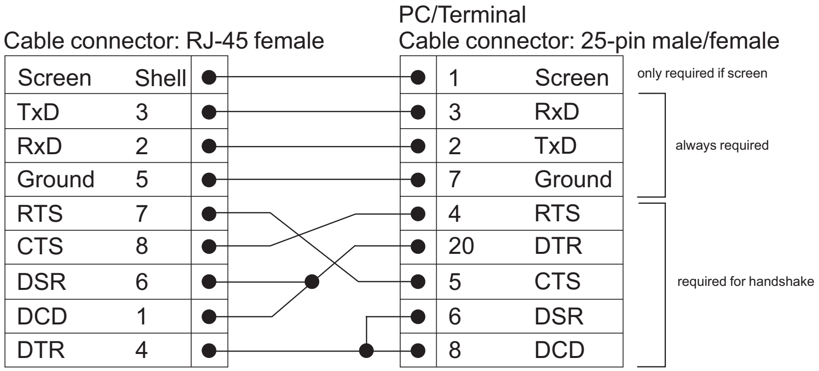
Table 13 Features of the OfficeConnect Managed Fast Ethernet PoE Switch (continued)

Feature	Description
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.

C PIN-OUTS

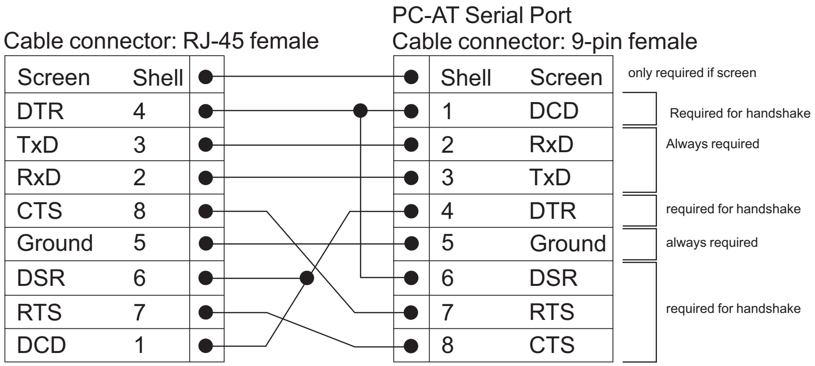
Null Modem Cable

RJ-45 to RS-232 25-pin



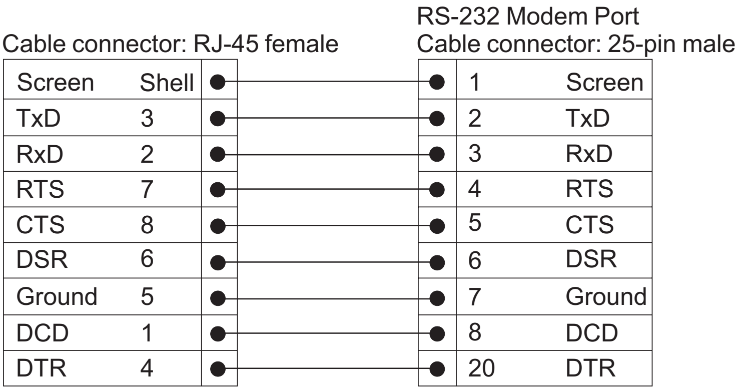
PC-AT Serial Cable

RJ-45 to 9-pin



Modem Cable

RJ-45 to RS-232 25-pin



Cable connector: RJ-45 female

RS-232 Modem Port
Cable connector: 25-pin male

Signal	RJ-45 pin	25-pin	Signal
Screen	Shell	1	Screen
TxD	3	2	TxD
RxD	2	3	RxD
RTS	7	4	RTS
CTS	8	5	CTS
DSR	6	6	DSR
Ground	5	7	Ground
DCD	1	8	DCD
DTR	4	20	DTR

Ethernet Port RJ-45 Pin Assignments

10/100 and 1000BASE-T RJ-45 connections.

Table 10 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 11 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–

D 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.
- **Fail Safe Commands** — Provides a way to recover from problems with firmware, configuration settings, or a lost user name or password.

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 20 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 Telnet or 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	Replace the serial cable
	Incorrect serial cable	Replace serial cable for a pin-to-pin straight/flat cable
	Software settings	Reconfigure the emulation software connection settings.
Response from the terminal emulations software is not readable	Faulty serial cable	Replace the serial cable
	Software settings	Reconfigure the emulation software connection settings.
Self-test exceeds 20 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	Configure the network address in the workstation
	No network address set	Configure the network address in the workstation
	Wrong or missing protocol	Configure the workstation with IP protocol
	Faulty Ethernet cable	Replace the cable
	Faulty port	Consult your technical support representative
	Faulty SFP transceiver	Replace the SFP transceiver
	Incorrect initial configuration	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

Problems	**Possible Cause**	**Solution**
No connection and the port LED is off	Incorrect Ethernet cable, e.g., crossed rather than straight cable, or vice versa, split pair (incorrect twisting of pairs)	Check pinout and replace if necessary
	Fiber optical cable connection is reversed	Change if necessary. Check Rx and Tx on fiber optic cable
	Bad cable	Replace with a tested cable
	Wrong cable type	Verify that all 100 Mbps connections use a Cat 5 cable
Lost Password		See "Fail Safe Commands"on page 241.

Fail Safe Commands

If the switch does not operate normally or if the firmware becomes corrupted, you can reset the switch and use the fail safe commands to resume operation by restoring the factory defaults, restoring the default user name and password, or downloading new firmware.

To enter fail safe mode:

1. Connect to the console interface as described in "Command Line Interface Management" on page 22.
2. Reboot the switch.
3. After the power-on self test completes and the runtime image finishes loading, the following message is displayed:.

```
Press Ctrl+C within 5 seconds to get into FailSafe mode
```

At this point, press Ctrl-C and wait for the remainder of the switch initialization to complete.

You will then be presented with options listed below.

- initialize – Deletes all stored configuration information, including IP address and address configuration mode, user names, and passwords. It then resets the switch to factory default settings, and restarts the system.

  Resetting the switch to factory defaults erases all your settings. You will need to reconfigure the switch after you reset it.

- password recovery – Deletes all user names and passwords, restores the default user names and passwords – "admin" with no password, and "monitor" with the same password, and then restarts the system.

- upgrade – Initiates a firmware download via TFTP. Follow the system prompts to specify the TFTP server where your firmware can be found, and then enter the source name of the firmware. After the file is downloaded, the system will be reset.

E Glossary

Access Control List (ACL) ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

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.

Boot Protocol (BOOTP) BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS) CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), or the DSCP priority bit.

Differentiated Services Code Point Service (DSCP) DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS) A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP) Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL) EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification.

EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

Generic Attribute Registration Protocol (GARP) GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3 Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet. (Now incorporated in IEEE 802.3-2005.)

IEEE 802.3ac Defines frame extensions for VLAN tagging.

IEEE 802.3af (PoE) An IEEE standard for providing Power over Ethernet (PoE) capabilities. When Ethernet is passed over copper cable, two twisted pairs are used for data transfer, and two twisted pairs are unused. With PoE, power can either be passed over the two data pairs or over the two spare pairs.

IEEE 802.3at (PoE Plus) An IEEE standard for providing more power to power-driven devices than the original Power over Ethernet (PoE) standard. When Ethernet is passed over copper cable, two twisted pairs are used for data transfer, and two twisted pairs are unused. With PoE Plus, power can either be passed over the two data pairs, the two spare pairs, or all four pairs depending on the capabilities of the attached device. Up to 30 Watts can be delivered through each port when using all four pairs.

IEEE 802.3u Defines CSMA/CD access method and physical layer specifications for 100BASE-TX and 100BASE-FX Fast Ethernet. (Now incorporated in IEEE 802.3-2005.)

IEEE 802.3x Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2005)

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query On each subnetwork, one IGMP-capable device can act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier is the device with the lowest IP address in the subnetwork.

Internet Control Message Protocol (ICMP) A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

Internet Group Management Protocol (IGMP) A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregated Group (LAG) Aggregates ports or VLANs into a single virtual port.

Link Aggregation See Port Trunk.

Management Information Base (MIB) An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message Digest Algorithm An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP) NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication See IEEE 802.1X.

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Power over Ethernet (PoE) Power over Ethernet provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources.

Remote Authentication Dial-in User Service (RADIUS) RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON) RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP) RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH) A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Network Management Protocol (SNMP) The application protocol in the Internet suite of protocols which offers network management services.

Spanning Tree Protocol (STP) A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Transmission Control Protocol/Internet Protocol (TCP/IP) Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP) A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP) UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN) A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

F OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

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.

TTroubleshoot 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 http://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	Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair			
Australia	1800 075 316	Philippines	1800 144 10220 or 029003078
Hong Kong	2907 0456	PR of China	800 810 0504
India	000 800 440 1193	Singapore	800 448 1433
Indonesia	001 803 852 9825	South Korea	080 698 0880
Japan	03 3507 5984	Taiwan	00801 444 318
Malaysia	1800 812 612	Thailand	001 800 441 2152
New Zealand	0800 450 454		

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	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	Norway	800 11376
Belgium	0800 71429	Poland	00800 4411 357
Denmark	800 17309	Portugal	800 831416
Finland	0800 113153	Russia	88005558588
France	0800 917959	Saudi Arabia	800 8 445 312
Germany	0800 182 1502	South Africa	0800 995 014
Hungary	06800 12813	Spain	900 938 919
Ireland	1 800 553 117	Sweden	020 795 482
Israel	180 945 3794	Switzerland	0800 553 072
Italy	800 879489	U.A.E.	04-3908997
Luxembourg	800 23625	U.K.	0800 096 3266
Netherlands	0800 0227788		
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 Contract requests: emea_contract@3com.com			

Country	Telephone Number	Country	Telephone Number
Latin America — Telephone Technical Support and Repair			
Antigua	AT&T +800 988 2112	Guatemala	AT&T +800 998 2112
Antigua Barbuda	AT&T +800 988 2112	Guyana	AT&T +800 998 2112
Argentina	AT&T +800 988 2112	Haiti	AT&T +800 998 2112
Aruba	AT&T +800 988 2112	Honduras	AT&T +800 998 2112
Bahamas	AT&T +800 988 2112	Jamaica	AT&T +800 998 2112
Barbados	AT&T +800 988 2112	Martinique	AT&T +800 998 2112
Belize	AT&T +800 988 2112	Mexico Mexico Local	1800 849 2273 +52-55-52-01-0004
Bermuda	AT&T +800 988 2112	Monserrat	AT&T +800 998 2112
Bolivia	AT&T +800 988 2112	Nicaragua	AT&T +800 998 2112
Brasil Brasil Local	0800-133266 (0800-13-3COM) +5511 5643 2700	Panama	AT&T +800 998 2112
British Virgin Islands	AT&T +800 988 2112	Paraguay	AT&T +800 998 2112
Cayman Islands	AT&T +800 988 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 988 2112	Puerto Rico	AT&T +800 998 2112
Colombia Colombia Local	AT&T +800 988 2112 +571 592 5000	Rest of Latin America	AT&T +800 998 2112
Costa Rica	AT&T +800 988 2112	St. Kitts Nevis	AT&T +800 998 2112
Curacao	AT&T +800 988 2112	St. Lucia	AT&T +800 998 2112
Dominican Republic	AT&T +800 988 2112	Suriname	AT&T +800 998 2112
Ecuador	AT&T +800 988 2112	Trinidad and Tobago	AT&T +800 998 2112
El Salvador	AT&T +800 988 2112	Turks and Caicos	AT&T +800 998 2112
French Guyana	AT&T +800 988 2112	Uruguay - Montivideo	AT&T +800 998 2112
Grenada	AT&T +800 988 2112	Venezuela	AT&T +800 998 2112
Guadalupe	AT&T +800 988 2112	Virgin Islands	AT&T +800 998 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, send e-mail to: `lat_support_anc@3com.com`

Country	Telephone Number	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	

REGULATORY NOTICES

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation.

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 B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe B 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 B 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 PoE Switch (3CRDSF9PWR) at http://www.3Com.com.

Also available at http://support.3com.com/doc/3CRDSF9PWR_EU_DOC.pdf

VCCI STATEMENT

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。

取り扱い説明書に従って正しい取り扱いをして下さい。