



3Com® Baseline Switch 2948-SFP Plus

User Guide

3CBLSG48

www.3Com.com

Part Number 10016089 Rev. AA

Published July 2007

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

Copyright © 2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

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® Baseline Switch 2948-SFP Plus. 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 Switch 2948 and how they 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.
- **General 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 & Query**— 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 DSCP and CoS mapping, policies, and configuring Trust mode.
- **Managing System Files** — Provides information for defining file maintenance.
- **Viewing Statistics** — Provides information for viewing RMON and interface statistics.
- **Managing Device Diagnostics** — Provides information for managing device diagnostics.




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

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

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com Web site:
■ <http://www.3Com.com>

Conventions Table 1 lists conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information 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	Warning Information that alerts you to potential Personal injury.

Related Documentation In addition to this guide, other documentation available for the 3Com Baseline Switch 2948 includes:
■ *Safety and Support Information*: Provides installation, set-up, and regulatory compliance information.

CONTENTS

1 GETTING STARTED

About the Switch 2948	2
Front Panel Detail	3
LED Status Indicators	4
System Specifications	5
Installing the Switch	6
Setting Up for Management	7
Methods of Managing a Switch	8
Switch Setup Overview.....	10
Using the Command Line Interface (CLI).....	14
Setting Up Web Interface Management.....	18
Setting Up SNMP Management V1 or V2	19
Default Users and Passwords	20
Upgrading Software using theCLI	20

2 USING THE 3COM WEB INTERFACE

Starting the 3Com Web Interface	21
Understanding the 3Com Web Interface	23
Saving the Configuration	31
Resetting the Device.....	32
Restoring Factory Defaults	34
Logging Off the Device.....	35

3	VIEWING BASIC SETTINGS	
	Viewing Device Settings	36
	Viewing Color Keys	38
4	MANAGING DEVICE SECURITY	
	Configuring System Access	41
	Defining RADIUS Clients.....	46
	Defining Port-Based Authentication (802.1X)	48
	Defining Access Control Lists.....	53
	Viewing Broadcast Storm	80
5	GENERAL SYSTEM INFORMATION	
	Viewing System Description	84
	Configuring System Name Information.....	86
	Configuring System Time	87
6	CONFIGURING PORTS	
	Viewing Port Settings	90
	Defining Port Settings	93
	Viewing Port Details	95
7	AGGREGATING PORTS	
	Viewing Link Aggregation	98
	Configuring Link Aggregation	99
	Modifying Link Aggregation	100
	Removing Link Aggregation	102

Viewing LACP	103
Defining LACP Priority	104
Defining LACP Port	105

8 CONFIGURING VLANS

VLAN Overview	106
Viewing VLAN Details.....	108
Viewing VLAN Port Details	109
Creating VLANs.....	110
Rename the VLANS	111
Modifying VLAN Settings	112
Modifying Port VLAN Settings	114
Removing VLANs.....	115

9 CONFIGURING IP AND MAC ADDRESS INFORMATION

Defining IP Addressing	117
Configuring ARP Settings	118
Viewing ARP Settings	119
Defining ARP Settings	120
Removing ARP Entries	121
Configuring Address Tables	122
Viewing Address Table Settings	123
Viewing Port Summary Settings	125
Adding Entries into Address Tables	126
Defining Aging Time	128
Removing Address Table Ports	129
Remove address Table	130

10 CONFIGURING IGMP SNOOPING & QUERY

Introduction	132
Defining IGMP Snooping & Query	132

11 CONFIGURING SPANNING TREE

Viewing Spanning Tree	136
Defining Spanning Tree	138
Modifying Spanning Tree.....	139

12 CONFIGURING SNMP

SNMP v1 and v2c	142
Defining SNMP Communities	143
Removing SNMP Communities	145
Defining SNMP Traps.....	146
Removing SNMP Traps.....	147

13 CONFIGURING QUALITY OF SERVICES

Viewing CoS Settings	150
Defining CoS	151
Defining Queuing Algorithm	152
Viewing CoS to Queue	153
Defining CoS to Queue	153
Viewing DSCP to CoS.....	155
Configuring DSCP to CoS	156
Configuring Trust Settings	157
Viewing Bandwidth Settings.....	158
Defining Bandwidth Settings	159
Defining Voice VLAN	161

14	MANAGING SYSTEM FILES	
	Configuration File Structure.....	170
	Backing Up System Files	171
	Restoring Files	172
	Upgrade the Firmware Image	173
	Activating Image Files.....	174

15	VIEWING STATISTICS	
	Viewing Port Statistics	175

16	MANAGING DEVICE DIAGNOSTICS	
	Configuring Port Mirroring	178
	Viewing Cable Diagnostics	181

A	3Com NETWORK MANAGEMENT	
	3Com Network Supervisor	184
	3Com Network Director	185
	3Com Network Access Manager	185
	3Com Enterprise Management Suite	186
	Integration Kit with HP OpenView Network Node Manager.....	186

B	DEVICE SPECIFICATIONS AND FEATURES	
	Related Standard.....	187
	Environmental.....	187
	Physical	187
	Electrical	188
	Switch Features.....	188

C	PIN-OUTS	
	Console Cable	193
	Null Modem Cable	194
	PC-AT Serial Cable	194
	Modem Cable	194
	Ethernet Port RJ-45Pin Assignments	195

D	TROUBLESHOOTING	
	Problem Management.....	196
	Troubleshooting Solutions	196

E	3Com CLI REFERENCE GUIDE	
	Getting Started with the Command Line Interface.....	199
	CLI Commands	200

F	GLOSSARY	
	210

G	OBTAINING SUPPORT FOR YOUR 3Com PRODUCTS	
	Register Your Product to Gain Service Benefits.....	216
	Solve Problems Online	216
	Purchase Extended Warranty and Professional Services	216
	Access Software Downloads.....	217
	Contact Us.....	217
	Telephone Technical Support and Repair	217

REGULATORY NOTICES

1

GETTING STARTED

This chapter contains introductory information about the 3Com® Baseline Switch 2948-SFP Plus and how they can be used in your network. It covers summaries of the hardware and software features, and the following topics:

- About the Switch 2948
- Front Panel Detail
- LED Status Indicators
- System Specifications
- Installing the Switch
- Setting Up for Management
- Methods of Managing a Switch
- Switch Setup Overview
- Using the Command Line Interface (CLI)
- Setting Up Web Interface Management
- Setting Up SNMP Management V1 or V2
- Default Users and Passwords
- Upgrading Software using the CLI

About the Switch 2948

The Switch 2948 is a Gigabit Ethernet switching product that delivers flexible three-speed performance (10/100/1000) and advanced voice-optimized features such as auto-QoS and auto-voice VLAN. This makes the switch ideal for medium businesses and small enterprises seeking to build a secure converged network.

The Switch 2948 includes the following model:

- Baseline Switch 2948-SFP Plus 48-Port

The Switch 2948 features the following advantages:

- Full Gigabit speed access ports
- Jumbo frames
- Port security
- Link aggregation control protocol (LACP)
- Up to 256 VLANs
- Access control lists (ACLs)
- Port-based mirroring

Summary of Hardware Features

Table 1 summarizes the hardware features supported by the Switch 2948.

Table 1 Hardware Features

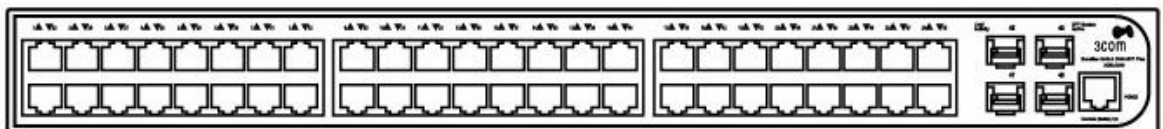
Feature	Switch 2948
Addresses	Up to 8,000 supported
Auto-negotiation	Supported on all ports
Forwarding Modes	Store and Forward
Duplex Modes	Half and full duplex on all front panel ports
Auto MDI/MDIX	Supported on all ports. If fiber SFP transceivers are used, Auto MDIX is not supported.

Table 1 Hardware Features (continued)

Feature	Switch 2948
Flow Control	In full duplex operation, all ports are supported. The Switch 2948 ports are capable of receiving, but not sending pause frames.
Traffic Prioritization	Supported (using the IEEE Std 802.1D, 1998 Edition): Four traffic queues per port
Ethernet, Fast and Gigabit Ethernet Ports	Auto-negotiating 10/100/1000BASE-T ports
SFP Ethernet Ports	Supports fiber Gigabit Ethernet long-wave (LX), and fiber Gigabit Ethernet short-wave (SX) transceivers in any combination.
Mounting	19-inch rack or standalone mounting

Front Panel Detail

Figure 1 shows the front panel of the Switch 2948-SFP Plus 48-Port unit.

Figure 1 Switch 2948 SFP 48-Port—front panel

LED Status Indicators

The 2948-SFP Plus 48-Port Ethernet switches provide LED indicators on the front panel for your convenience to monitor the switch.

Table 2 Describes the meanings of the LED.

Table 2 Description on the LEDs of the Switch 2948

LED	Label	Status	Description
Power	Power	Green	The switch starts normally. The LED flashes when the system is performing power-on self test (POST).
		Yellow	The system has entered the fail safe mode. The LED flashes when the system has failed the POST.
		OFF	The switch is powered off.
10/100/1000 Mbps; BASE-T Ethernet port status	Link/ Activity	Green	The port works at the rate of 1000. 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.
1000Base SFP 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.
		OFF	The port is not connected.
	Module	Green	The SFP module is inserted.
	Active	OFF	The SFP module is not inserted or is not recognized.

System Specifications

Table 3 contains the system specifications of the Switch 2948.

Table 3 System specifications of the Switch 2948 switch

Specification	Switch 2948-SFP Plus 48-Port 3CBLSG48
Physical dimensions (H×W×D)	44×440×265 mm (1.73 X 17.3 X 10.43 in.)
Weight	2.0 kg (4.4 lbs)
Console port	One Console port
Gigabit Ethernet ports on the front panel	48 × 10/100/100 Mbps Ethernet ports; Four Gigabit SFP Combo ports
AC Input voltage	Rated voltage range: 100–240 VAC, 50/60 Hz
Power consumption (full load)	70 W
Operating temperature	0 to 40 °C (32 to 113 °F)
Relative humidity	10 to 90% non-condensing

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

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



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



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



VORSICHT: Sicherheitsinformationen. Bevor Sie Komponenten aus dem Switch entfernen oder den Switch hinzufügen 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.



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



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

Setting Up for Management

To make full use of the features offered by your switch, and to change and monitor the way it works, you have to access the management software that resides on the switch. This is known as managing the switch. Managing the switch can help you to improve the efficiency of the switch and therefore the overall performance of your network. This section explains the initial set up of the switch and the different methods of accessing the management software to manage a switch. It covers the following topics:

- Methods of Managing a Switch
- Switch Setup Overview
- Manually set the IP Address using the Console Port
- Viewing IP Information using the Console Port
- Setting Up Web Interface Management
- 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:

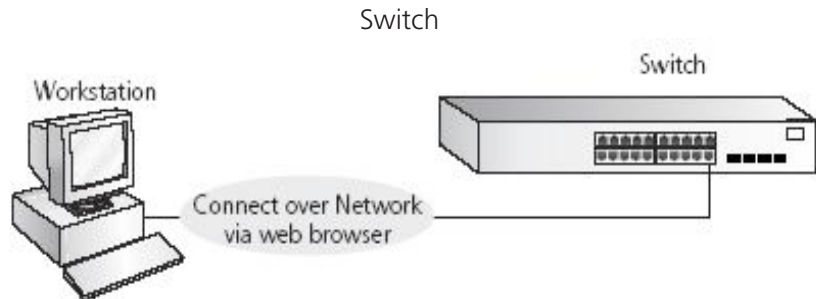
- Web Interface Management
- SNMP Management

In addition, you can use the Command Line Interface through the Console port for basic operations of the switch including setting and viewing the IP address, configuring user accounts, upgrading switch firmware, and more. Refer to “3Com CLI Reference Guide” on page 195.

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).

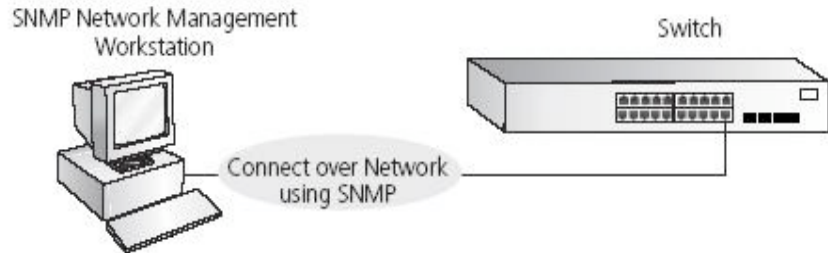
Figure 2 Web Interface Management over the Network



Refer to “Setting Up Web Interface Management” on page 18.

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

Figure 3 SNMP Management over the Network

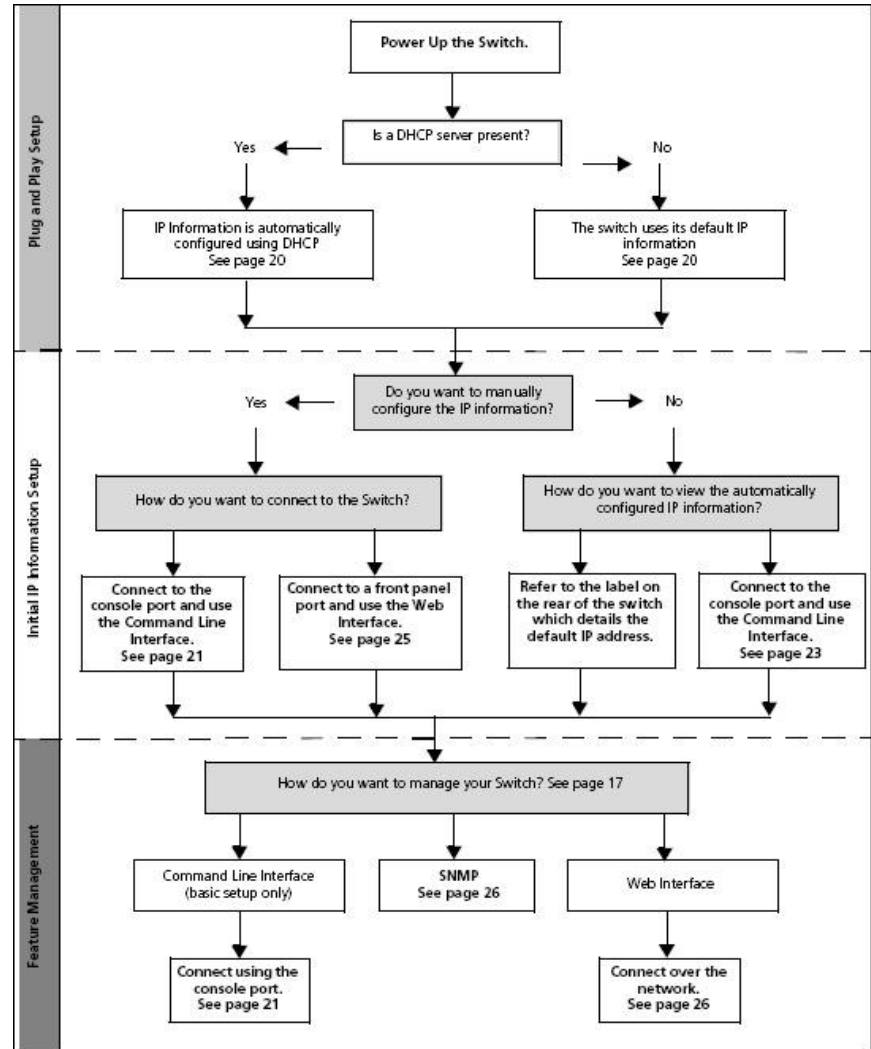


Refer to "Setting Up SNMP Management V1 or V2" on page 19.

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 4. 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 4 Initial Switch Setup and Management Flow Diagram

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 20.

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 rear 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 17.

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 16.

Using the Command Line Interface (CLI)

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



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

Connecting to the Console Port

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

Prerequisites

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

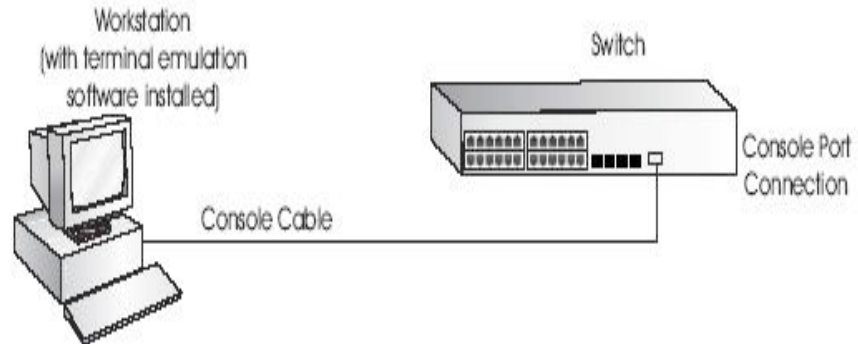


You can find pin-out diagrams for the cable in Appendix C.

Connecting the Workstation to the Switch

1 Connect the workstation to the console port using the console cable as shown in Figure 5.

Figure 5 Connecting a Workstation to the Switch using the Console Port



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 Switch 2948 takes approximately one minute to boot.

Manually set the IP Address using the Console Port

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

■ You need to have the following information:

- IP address
- subnet mask
- default gateway

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

2 The command line interface login sequence begins as soon as the switch detects a connection to its console port. When the process completes, the Login prompt displays.

3 At the **login** prompt, enter **admin** as your user name and press Return. The **Password** prompt displays.

4 Press Return. If you have logged on correctly, **Select menu option:** should be displayed.

5 Enter the IP address and subnet mask for the switch as follows:

Select menu option: ipSetup

Enter configuration method (auto,manual): manual

Enter IP address [169.254.145.76]:xxx.xxx.xxx.xxx

Enter subnet mask [255.255.0.0]:mmm.mmm.mmm.mmm

Enter gateway IP address [0.0.0.0]:ggg.ggg.ggg.ggg

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

6 Enter the **logout** 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 8.

Viewing IP Information using the Console Port

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

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

The automatic IP configuration process usually completes within one minute.

2 The command line interface login sequence begins as soon as the switch detects a connection to its console port.

3 At the login prompt, enter **admin** as your user name and press Return.

4 At the password prompt, press Return. If you have logged on correctly, **Select menu option:** is displayed.

5 Enter **Summary** to view a summary of allocated IP addresses. The following is an example of the display from the Summary command.

```
Select menu option: summary
IP Method:          Manual
IP address:         169.254.145.76
Subnet mask:        255.255.0.0
Default gateway:    0.0.0.0
Runtime version:    00.00.29
Bootcode version:   00.00.12
Select menu option:
```

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 8.



For more information about the CLI, refer to “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 logout, disconnect the serial cable and close the terminal emulator software.

Setting Up Web Interface Management

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

Prerequisites

- Ensure that you have already set up the switch with IP information as described in “Methods of Managing a Switch” on page 8.
- 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 6	Yes	Yes	Yes
Internet Explorer 7	Yes	Yes	Yes
Firefox 1.5	Yes	Yes	Yes
Firefox 2	Yes	Yes	Yes
Netscape 8	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 12, and "Viewing IP Information using the Console Port" on page 17.

2 Check that your management workstation is on the same subnet as your switch.

3 Check you can communicate with the switch by entering a **ping** command at the DOS or CMD prompt in the following format:

c:\ ping xxx.xxx.xxx.xxx

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

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

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

http://xxx.xxx.xxx.xxx

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

The main Web interface page is displayed.

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".

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. Note that the management workstation does not have to be physically connected to the switch.

To display and configure SNMP management parameters, refer to "Configuring SNMP" in Chapter 12.

Default Users and Passwords

If you intend to manage the switch or to change the default passwords, you must log in with a valid user name and password. The switch has one default user name. The default user is listed in Table 5.

Table 5 Default Users

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



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

Upgrading 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 “Upgrade the Firmware Image”. Bootcode can only be upgraded using the CLI.

1 To download the runtime application file, enter:

```
Select menu option: upgrade
TFTP Server Address [0.0.0.0]:
File Name [bprxx_yy_zz.bin]:
```

Then follow the prompt to enter the IP address of the TFTP server and the source runtime filename.

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

reboot

The following prompt displays:

Are you sure you want to reboot the system (yes, no):

3 Enter **yes** 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
- 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 Section. Login information is always handled in the local database. A unique password is required from 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 6 Enter Network Password Page

Baseline Switch 2948-SFP Plus

3COM

3CBLSG48 Login

User Name

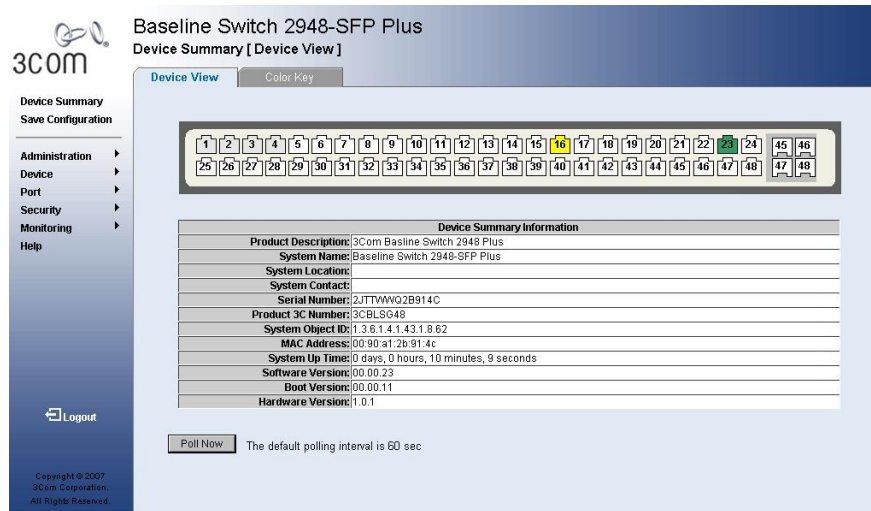
Password

Login

Copyright © 2007
3Com Corporation
All Rights Reserved

- 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:

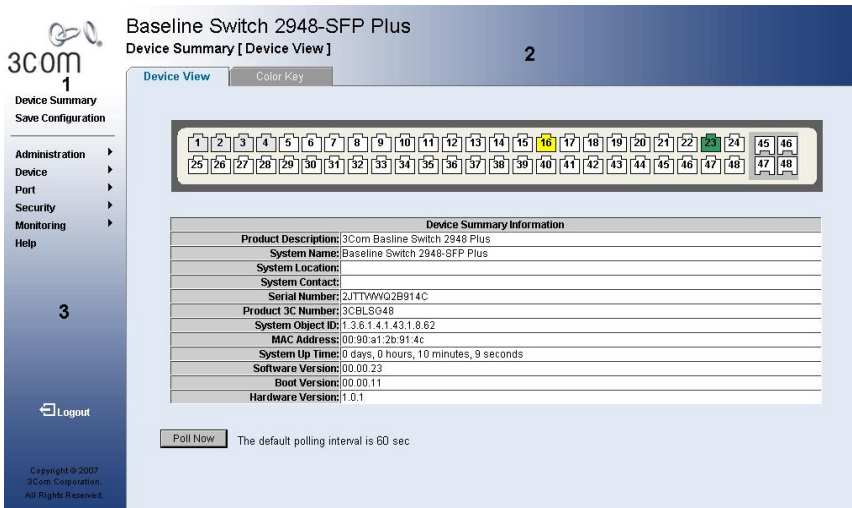
Figure 7 3Com Web Interface Home Page

Understanding the 3Com Web Interface

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

- **Tab View** — Provides the device summary configuration located at the top of the home page.
- **Tree View** — Provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
- **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 8 Web Interface Components



The following table lists the user interface components with their corresponding numbers:

Table 6 Interface Components

View	Description
1 Tree View	Tree View provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
2 Tab View	The Tab Area enables navigation through the different device features. Click the tabs to view all the components under a specific feature.
3 Web Interface	Provides access to online help, and contains information about Information 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 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 9 Device Representation



- 2 By selecting a specific port with your mouse, you can view the Detail port, Setup, and Statistics.

For detailed information on configuring ports, refer to "Configuring Ports" on page 90.

Using the Web Interface Management Buttons

Configuration Management buttons and icons provide an easy method of configuring device information:

Table 7 3Com Web Interface Configuration Buttons

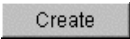
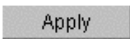
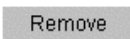
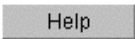

Button	Button Name	Description
	Create	Creates configuration entries.
	Apply	Applies configuration changes to the device.
	Delete	Deletes configuration settings.

Table 8 3Com Web Interface Information Tabs

Tab	Tab Name	Description
	Help	Opens the online help.
	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 10 Port Settings Summary Page

Baseline Switch 2948-SFP Plus
Port > Administration [Summary]

Summary Detail Setup

Port	State	Flow Control	Speed	Duplex	PVID
1	Disabled	Disabled	Auto	Auto	1
2	Enabled	Disabled	Auto	Auto	1
3	Disabled	Disabled	Auto	Auto	1
4	Enabled	Disabled	Auto	Auto	1
5	Enabled	Disabled	1000M	Full	1
6	Enabled	Disabled	100M	Full	1
7	Enabled	Enabled	100M	Half	1
8	Enabled	Disabled	10M	Full	1
9	Enabled	Enabled	10M	Half	1
10	Enabled	Disabled	Auto	Auto	1
11	Enabled	Disabled	Auto	Auto	1
12	Enabled	Disabled	Auto	Auto	1
13	Enabled	Disabled	Auto	Auto	1
14	Enabled	Disabled	Auto	Auto	1
15	Enabled	Disabled	Auto	Auto	1
16	Enabled	Disabled	Auto	Auto	1
17	Enabled	Disabled	Auto	Auto	1
18	Enabled	Disabled	Auto	Auto	1
19	Enabled	Disabled	Auto	Auto	1
20	Enabled	Disabled	Auto	Auto	1
21	Enabled	Disabled	Auto	Auto	1
22	Enabled	Disabled	Auto	Auto	1
23	Enabled	Disabled	Auto	Auto	1

Device Summary
Save Configuration

Administration >
Device >
Port >
Security >
Monitoring >
Help

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

Adding Configuration Information

The *IP Setup Page* enables you to add User-defined information to specific 3Com Web Interface pages.

For example, to configure IP Setup:

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

Figure 11 IP Setup Page

The screenshot displays the 3Com web interface for a Baseline Switch 2948-SFP Plus. The left sidebar contains a navigation menu with options: Device Summary, Save Configuration, Administration (selected), Device, Port, Security, Monitoring, and Help. The main content area is titled 'IP Setup' and shows the 'Configuration Method' section with two radio buttons: 'Static' (selected) and 'DHCP'. Below this, there are input fields for 'IP Address' (169.254.145.76), 'Subnet Mask' (255.255.0.0), and 'Gateway'. At the bottom of the page, there are 'Help', 'Apply', and 'Cancel' buttons. The footer includes copyright information for 3Com Corporation.

2 Enter the 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 12 System Access Modify Page

Baseline Switch 2948-SFP Plus
Administration > System Access [Modify]

Summary Setup **Modify** Remove

Users Summary

User Name	Access Level
admin	Management
Monitor	Monitor

Access Level:

☐ Password Modify

Password: (8 Character Maximum) Confirm Password:

Help Apply Cancel

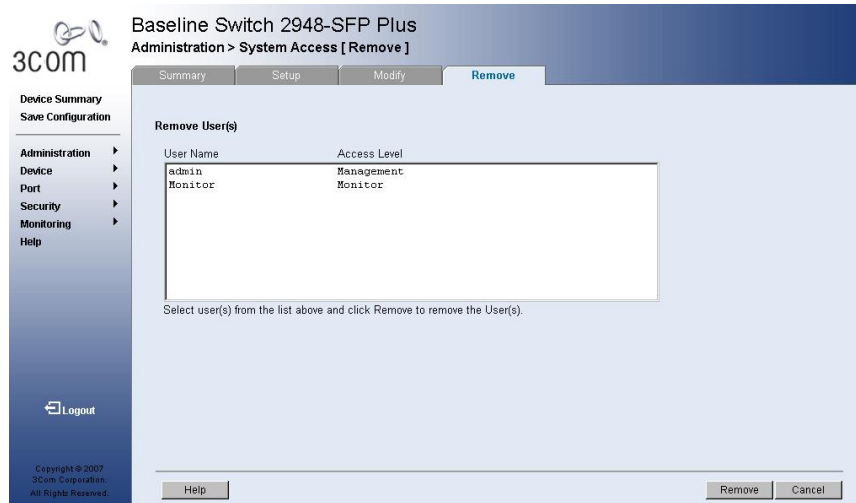
2 Modify the fields.

3 Click **Apply**. The access fields are modified.

Removing Configuration Information

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

Figure 13 System Access Remove Page



2 Select the user account to be deleted.

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

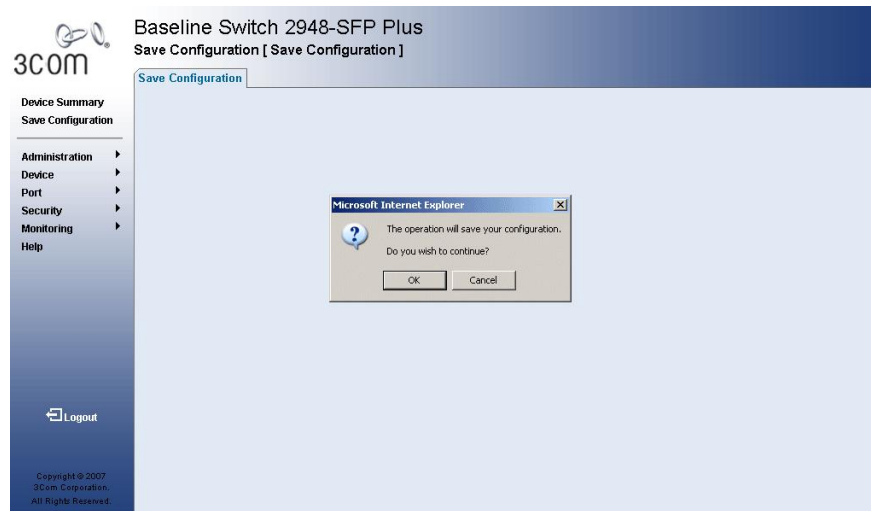
Saving the Configuration

Configuration changes are only saved to the device once the user saves the changes to the flash memory. The Save Configuration tab 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 14 Save Configuration Page



A message appears: *The operation will save your configuration. Do you wish to continue?*

2 Click **OK**. A message appears: *Configuration is saved to flash memory successfully.*

The configuration is saved.

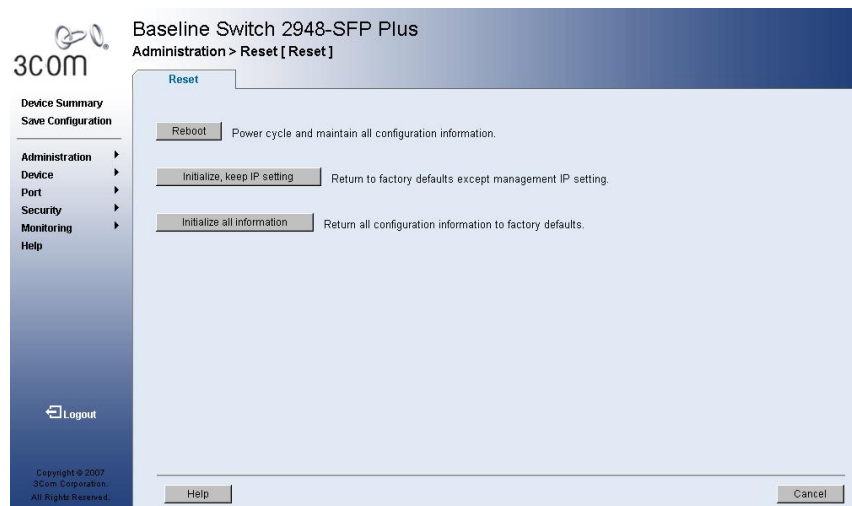
Resetting the Device

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 15 Reset Page



2 Click **Reboot**. A confirmation message is displayed.

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

Figure 16 User Name and Password Page

The image shows a login form titled "3CBLSG48 Login" in a dark blue header. Below the header, there are two input fields: "User Name" and "Password". The "User Name" field is a simple text box, while the "Password" field is a text box with a small icon on the right side, likely for password visibility. Below these fields is a "Login" button.

3CBLSG48 Login	
User Name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

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

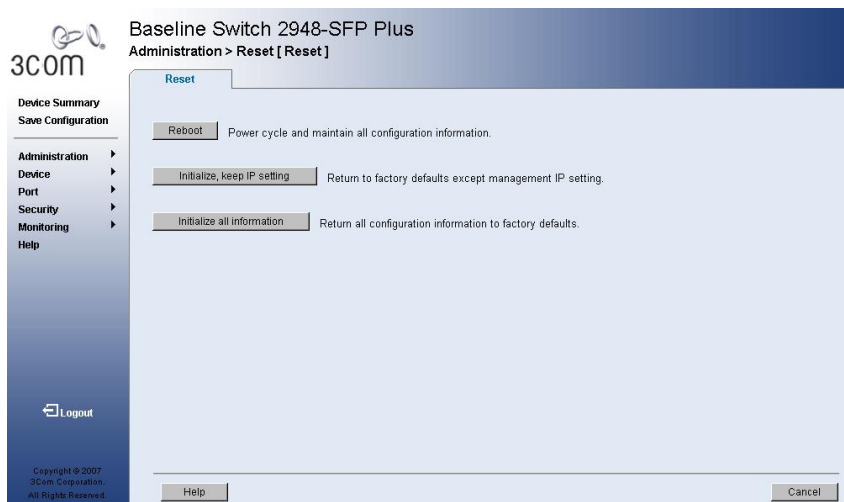
Restoring Factory Defaults

The Restore option appears on the *Reset Page*. The Restore option restores the device to its factory default settings.

To restore the device:

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

Figure 17 Reset Page



The *Reset Page* contains the following fields:

- **Initialize with Current IP Address** — Resets the device with the factory default settings, but maintains the current IP Address, subnet mask, and default gateway address.
- **Initialize with Default IP Address** — Resets the device with the factory default settings, including the factory default IP Address.

- 2 Click the **Initialize** button. The system is restored to factory defaults.

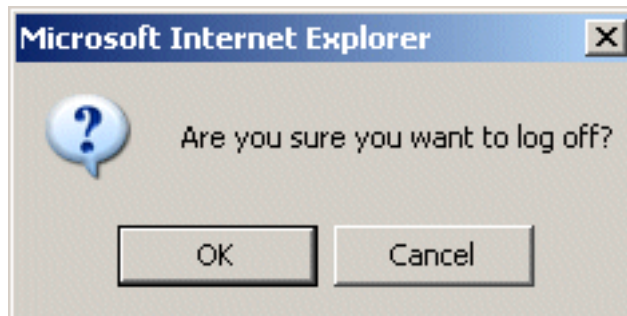
Logging Off the Device

To log off the device:

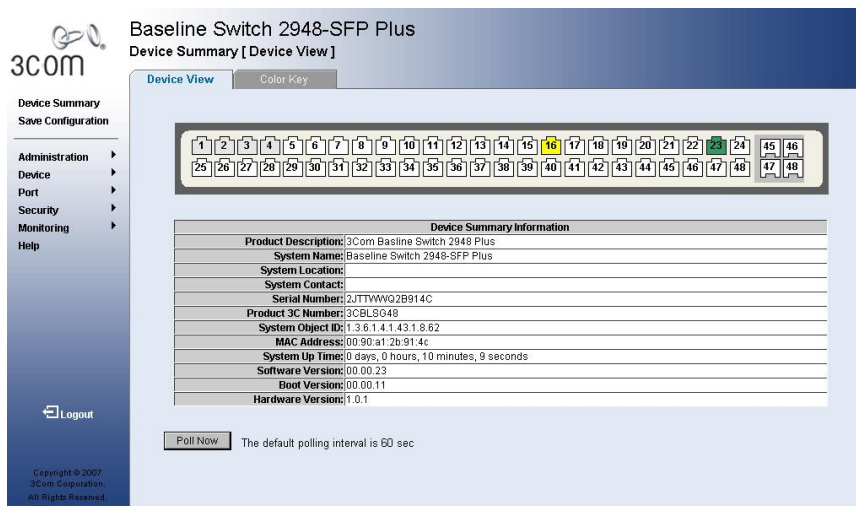
- 1 Click **Logout**. The *Logout Page* opens.



- 2 The following message appears:



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



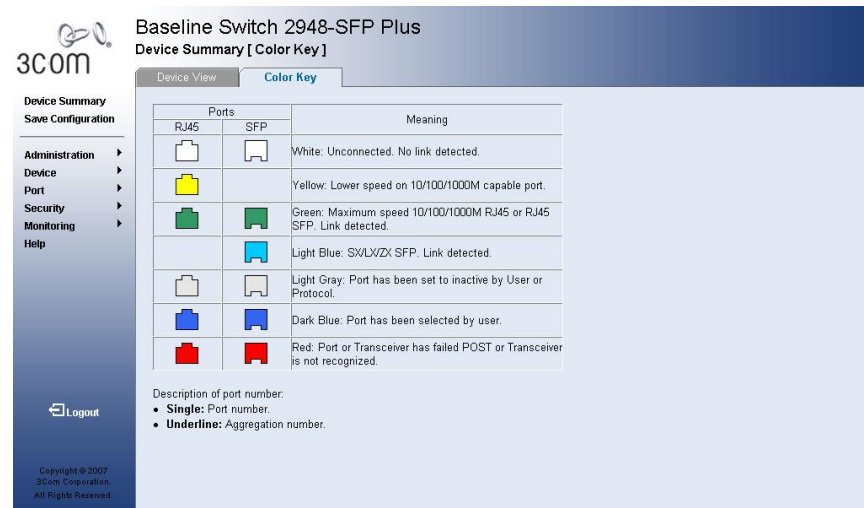
The Device Summary Page contains the following fields:

- **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.
- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **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.

Viewing Color Keys The *Color Key Page* provides information about the RJ45 or SFP port status. To view color keys:

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

Figure 19 Color Key Page



The *Color Key Page* contains the following fields:

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

Table 9 describes the color and the port status:

Table 9 Color Key Definitions

Color	Port Status
White	Unconnected. No link detected.
Yellow	Lower speed on 10/100/1000M port.
Green	Maximum speed 10/100/1000M RJ45 or RJ45 SFP. Indicates that a link was detected.
Light Blue	SX/LX 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 defining access control lists.

This section includes the following topics:

- Configuring System Access
- Defining RADIUS Clients
- Defining Port-Based Authentication (802.1X)
- Defining Access Control Lists
- Viewing Broadcast Storm

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 10 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 from 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 user name: 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

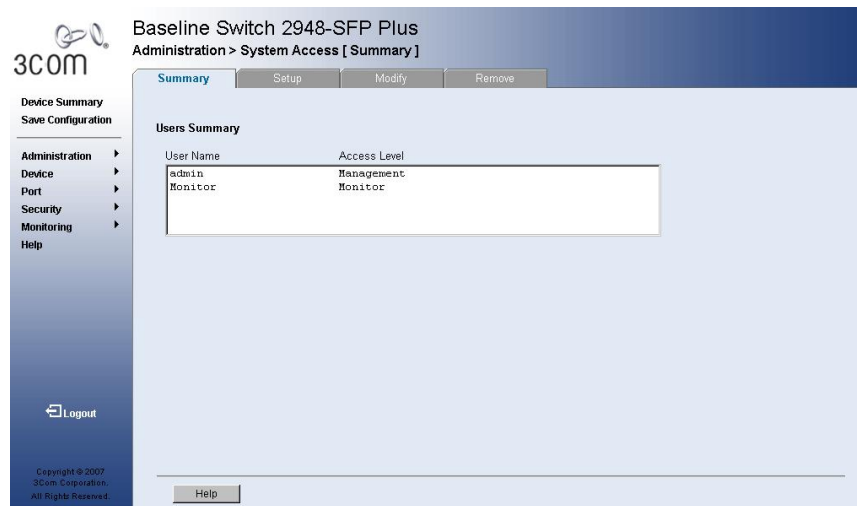
Viewing System Access Settings

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 20 System Access Summary Page



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

- **User Name** — Displays the user name. The possible predefined field value is:
 - *Admin* — Displays the predefined Administrative 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.

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

Figure 21 System Access Setup Page

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 8 characters.
- **Confirm Password** — Verifies the password.

2 Define the fields.

3 Click **Apply**. The Users are created, and the device is updated.

Modifying System Access

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

Monitor users have no access to this page.

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

Figure 22 System Access Modify Page

Baseline Switch 2948-SFP Plus
Administration > System Access [Modify]

Summary Setup **Modify** Remove

Users Summary

User Name	Access Level
admin	Management
monitor	Monitor

Access Level:

☐ Password Modify

Password:
(8 Character Maximum)

Confirm Password:

Help Apply Cancel

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

- **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.
 - *Monitor* — Provides users with read access rights.
- **Password Modify** — Changes a password for an existing user.
- **Password** — Defines the local user password. Local user passwords can contain up to 8 characters.
- **Confirm Password** — Verifies the password.

2 Select a User Name to be modified.

3 Modify the fields.

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

Removing System Access

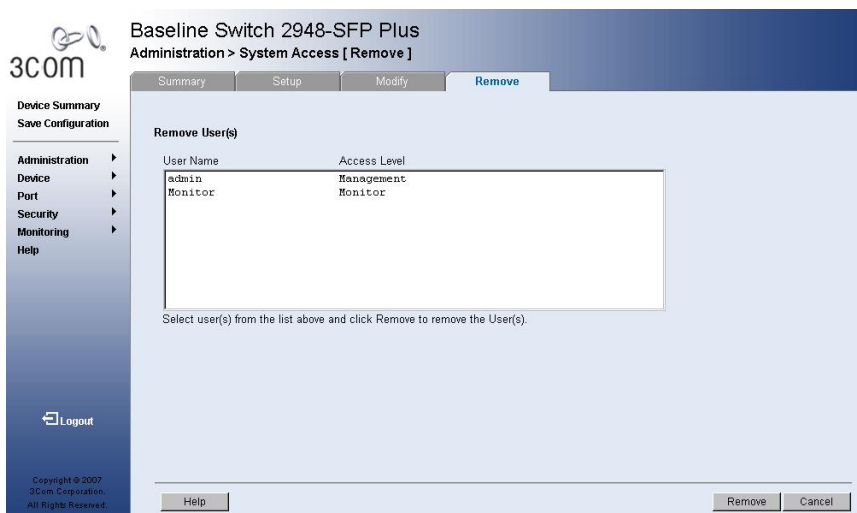
The *System Access Remove Page* allows network administrators to remove users from the System Access Interface.

Monitor users have no access to this page.

To remove users:

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

Figure 23 System Access Remove Page



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

- **Remove User(s)** — Select user(s) from the list below to be removed.
- **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 a *User* to be deleted.

The last user with management access may not be deleted.

3 Click **Remove**. The *User* is 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. The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

Monitor users have no access to this page.

To configure the RADIUS client:
1 Click **Security > RADIUS Client > Setup**. The *Radius Client Setup Page* opens.

Figure 24 Radius Client Setup Page

The screenshot shows the 'Radius Client Setup' page for a 3Com Baseline Switch 2948-SFP Plus. The page is titled 'Security > Radius Client [Setup]'. On the left, there is a navigation menu with options: Administration, Device, Port, Security, Monitoring, and Help. Below the menu is a 'Logout' button. The main content area is divided into two columns: 'Primary Server' and 'Backup Server'. Each column contains the following fields: Host IP Address (0.0.0.0), Authentication Port (1812), Number of Retries (3), Timeout for Reply (3 (Sec)), Dead Time (0 (Min)), and Key String (Alpha Numeric). At the bottom of the page, there are 'Help', 'Apply', and 'Cancel' buttons. The footer contains copyright information: 'Copyright © 2007 3Com Corporation. All Rights Reserved.'

The *Radius Client Setup Page* contains the following fields:

- **Primary Server** — Defines the RADIUS Primary Server authentication fields.
- **Backup Server** — Defines the RADIUS Backup Server authentication fields.
- **Host IP Address** — Defines the RADIUS Server IP address.

- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default value is 3.
- **Timeout for Reply** — 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 1-30. The default value is 3.
- **Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default value is 0.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.

2 Define the fields.

3 Click **OK**. 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 25 802.1X Summary Page



Baseline Switch 2948-SFP Plus
Security > 802.1x [Summary]

Port	User Name	Current Port Control	Guest VLAN	Periodic Reauthentication	Reauthentication Period	Authenticator State	Termination Cause
1	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
2	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
3	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
4	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
5	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
6	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
7	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
8	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
9	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
10	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
11	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet
12	N/A	Authorized	Disable	Disable	3600	Force Authorized	Not Terminated Yet

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

- **Port** — Displays a list of interfaces.
- **User Name** — Displays the supplicant user name.
- **Current Port Control** — Displays the current port authorization state.
- **Guest VLAN** — Indicates whether an unauthorized port is allowed to join the Guest VLAN. The possible field values are:
 - *Enabled* — Enables an unauthorized port to join the Guest VLAN.
 - *Disabled* — Disables an unauthorized port to join the Guest VLAN.
- **Periodic Reauthentication** — Enables periodic reauthentication on the port.
 - *Enabled* — Enables the periodic reauthentication on the port.
 - *Disabled* — Disables the periodic reauthentication 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.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

2 Click **Apply**. Port Authentication is enabled, and the device is updated.

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 setting for each port individually.

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 26 802.1X Setup Page

3Com Baseline Switch 2948-SFP Plus
Security > 802.1x [Setup]

Summary Setup

802.1x Global Settings

Port Based Authentication State: Disabled
Authentication Method: Radius
Enable Guest VLAN: ☒
Guest VLAN ID: 1

802.1x Port Settings

Admin Port Control: Force Authorized
Guest VLAN: Disabled
Periodic Authentication: Disabled
Reauthentication Period: 3600

Select Ports:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	45	46
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	47	48

Select All Select None

Help Apply Cancel

Copyright © 2007 3Com Corporation. All Rights Reserved.

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

802.1X Global Settings

- **Port Based Authentication State** — Indicates 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 value.
- **Authentication Method** — Specifies the authentication method used for port authentication. The possible field values are:
 - *RADIUS* — Provides port authentication using the RADIUS server.
 - *RADIUS, None* — Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
 - *None* — Indicates that no authentication method is used to authenticate the port.
- **Enable Guest VLAN** — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.
- **Guest VLAN ID** — Specifies the guest VLAN ID.

802.1X Port Settings

- **Admin Port Control** — Displays 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 resends 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.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the port. The possible field values are:
 - *Enabled* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected from the Guest VLAN ID dropdown list.
 - *Disabled* — Disables Guest VLAN on the port. This is the default.
- **Periodic Reauthentication** — Enables periodic reauthentication on the port.
 - *Enabled* — Enables the periodic reauthentication on the port.
 - *Disabled* — Disables the periodic reauthentication on the port.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.

2 Define the fields.

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

Defining Access Control Lists

Access Control Lists (ACL) 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. If they are denied entry, the port can be disabled.

For example, an ACL rule is defined states that port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is 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 the packets by the Source port IP address and wildcard mask.
- **Destination Port IP Address and Wildcard Mask** — Filters the packets by the Source port IP address and wildcard mask.
- **ACE Priority** — Filters the packets by the ACE priority.
- **Protocol** — Filters the packets by the IP protocol.
- **DSCP** — Filters the packets by the DiffServ Code Point (DSCP) value.
- **IP Precedence** — Filters the 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:

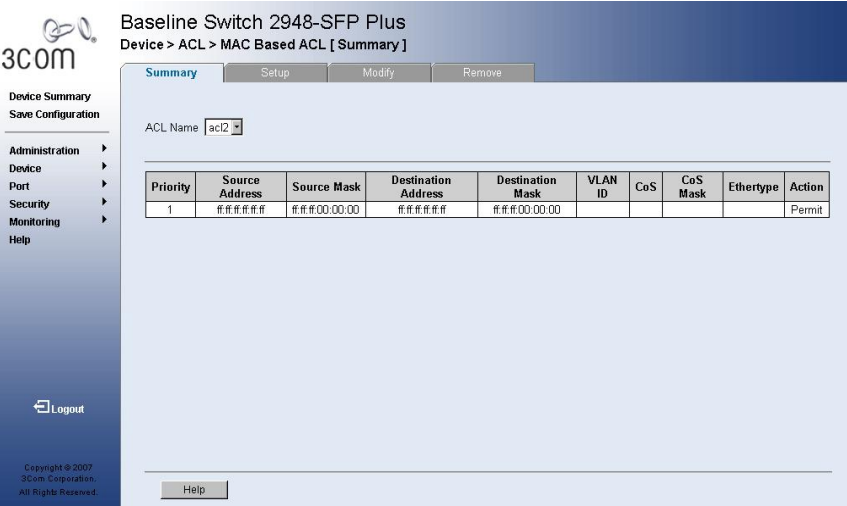
- Viewing MAC Based ACLs
- Configuring MAC Based ACLs
- Removing MAC Based ACLs
- Viewing IP Based ACLs
- Defining IP Based ACLs
- Modifying IP Based ACLs
- Removing IP Based ACLs
- Viewing ACL Binding
- Configuring ACL Binding
- Removing ACL Binding

Viewing MAC Based ACLs

The *MAC Based ACL Summary Page* displays information regarding MAC Based ACLs configured on the device. Ports are reactivated from the Interface Configuration Page.

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

Figure 27 MAC Based ACL Summary Page



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

- **ACL Name** — Contains a list of the MAC-based ACLs.
- **Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first match basis.
- **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 ACE. The possible field values are 1 to 4094.
- **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 among 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 select, create, and define rules for MAC-based Access Control Lists.

Monitor users have no access to this page.

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

Figure 28 MAC Based ACL Setup Page

Baseline Switch 2948-SFP Plus
Device > ACL > MAC Based ACL [Setup]

Summary Setup Modify Remove

Selection ACL: acl2 Create ACL Create

Add Rules to ACL:

Priority:

Source MAC Address: Source Mask: Any

Destination MAC Address: Destination Mask: Any

VLAN ID:

CoS: CoS Mask:

EtherType:

Action: Permit

Priority	Source Address	Source Mask	Destination Address	Destination Mask	VLAN ID	CoS	CoS Mask	EtherType	Action
1	#####	##00:00:00	#####	##00:00:00					Permit

Help Apply Cancel

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

- **Selection ACL** — Lists previously defined Access Control Lists.
- **Create ACL** — Create a new user-defined MAC based ACL.

Add Rules to ACL

- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-65535.
- **Source MAC Address** — Matches the source MAC address to which packets are addressed to the ACE.

- **Source Mask** — Indicates 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 no bit is important. A wildcard of 00:00:00:00:00:00 indicates that all bits are important.

For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, 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 to the ACE.
- **Destination Mask** — Indicates 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. A wildcard mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard mask of 00:00:00:00:00:00 indicates that all bits are important.

For example, if the destination MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the first five bytes of the MAC are used, while the last byte is ignored. For the destination 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 first five bytes of the MAC are used, while the last byte is ignored. For the destination 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.

- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4094.
- **CoS** — Classifies traffic based on the CoS tag value.
- **CoS Mask** — Defines the CoS mask used to classify network traffic.
- **Ethertype** — Provides an identifier that differentiates among 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.

2 Define the fields.

3 Click **Apply**. The Rule Setup settings are configured, and the device is updated.

Modifying MAC Based ACLs

The *MAC Based ACL Modify Page* allows the network administrator to modify MAC Based ACLs settings.
Monitor users have no access to this page.

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

Figure 29 MAC Based ACL Modify Page

Baseline Switch 2948-SFP Plus
Device > ACL > MAC Based ACL [Modify]

Summary Setup **Modify** Remove

Select ACL: **acl2**

Select Rule

Priority	Source Address	Source Mask	Destination Address	Destination Mask	VLAN ID	CoS	CoS Mask	Ethertype	Action
1	#####	#####	#####	#####					Permit

Modify Rule:

Priority:

Source MAC Address: ☒ Source Mask: ☐ Any

Destination MAC Address: ☒ Destination Mask: ☐ Any

VLAN ID:

CoS: CoS Mask:

Ethertype:

Action: **Permit**

Help Apply Cancel

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

- **Select ACL** — Selects the ACL to be bound.
- **Select Rule** — Indicates the rule for which Access Control Entries are defined.

Modify

- **Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first match basis.
- **Source MAC Address** — Matches the source MAC address to which packets are addressed to the ACE.
- **Source Mask** — Indicates the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source address by specifying which bits are used and which are ignored. A wildcard

mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard of 00:00:00:00:00:00 indicates that all bits are important. For example, if the source MAC address is E0:3B:4A:C2:CA:E2 and the wildcard mask is 00:00:00:00:00:FF, the first five bytes of the MAC are used, while the last byte is ignored. For the source MAC address E0:3B:4A:C2:CA:E2, this wildcard mask matches all MAC addresses in the range E0:3B:4A:C2:CA:00 to E0:3B:4A:C2:CA:FF.

- **Destination MAC Address** — Matches the destination MAC address to which packets are addressed to the ACE.
- **Destination Mask** — Indicates the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination address by specifying which bits are used and which are ignored. A wildcard mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard mask of 00:00:00:00:00:00 indicates that all bits are important.. For example, if the destination MAC address is E0:3B:4A:C2:CA:E2 and the wildcard mask is 00:00:00:00:00:FF, the first five bytes of the MAC are used, while the last byte is ignored. For the destination MAC address 0:3B:4A:C2:CA:E2, this wildcard mask matches all MAC addresses in the range E0:3B:4A:C2:CA:00 to E0:3B:4A:C2:CA:FF.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4094
- **CoS** — Classifies traffic based on the CoS tag value.
- **CoS Mask** — Defines the CoS mask used to classify network traffic.
- **Ethertype** — Provides an identifier that differentiates among 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.

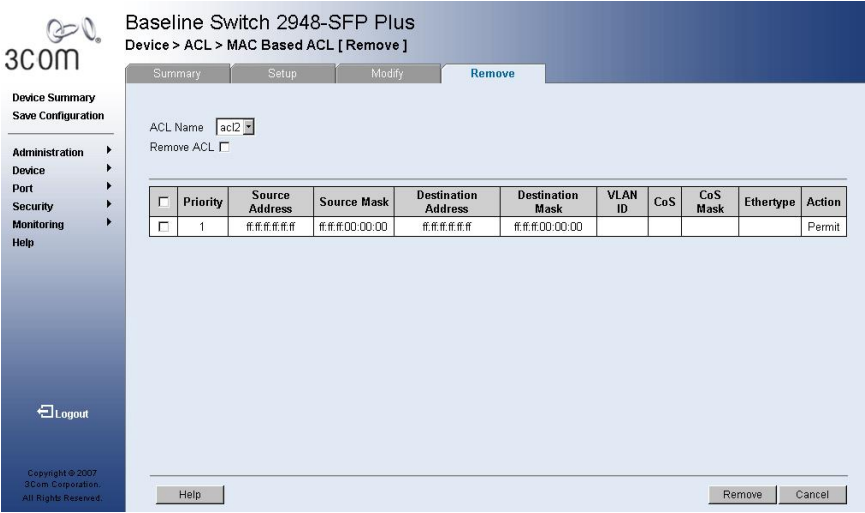
- 2 Define the fields.
- 3 Click **Apply**. The Rule Setup settings are configured, and the device is updated.

Removing MAC Based ACLs

The *MAC Based ACL Remove Page* allows the user to remove MAC Based ACLs.
Monitor users have no access to this page.

To remove MAC Based ACLs:
1 Click **Device > ACL > MAC Based ACL > Remove**. The *MAC Based ACL Remove Page* opens.

Figure 30 MAC Based ACL Remove Page



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

- **ACL Name** — Contains a list of the MAC-based ACLs.
- **Remove ACL** — Enables the ACL to be removed.
- **Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first match basis.

- **Source Address** — Matches the source MAC address to which packets are addressed to the ACE.
- **Source Mask** — Indicates 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 no bit is important. A wildcard of 00:00:00:00:00:00 indicates that all bits are important.

For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, 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 Address** — Matches the destination MAC address to which packets are addressed to the ACE.
- **Destination Mask** — Indicates 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. A wildcard mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard mask of 00:00:00:00:00:00 indicates that all bits are important.

For example, if the destination MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the first five bytes of the MAC are used, while the last byte is ignored. For the destination 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 first five bytes of the MAC are used, while the last byte is ignored. For the destination 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.

- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4094.
 - **CoS** — Classifies Class of Service of the packet.
 - **CoS Mask** — Defines the wildcard bits to be applied to the CoS.
 - **Ethertype** — Provides an identifier that differentiates among 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.
- 2 Select the ACL Name to be deleted.
 - 3 Select the ACL to be removed from the table.
 - 4 Click the Remove checkbox.
 - 5 Click **Apply**. The selected ACLs are deleted, and the device is updated.

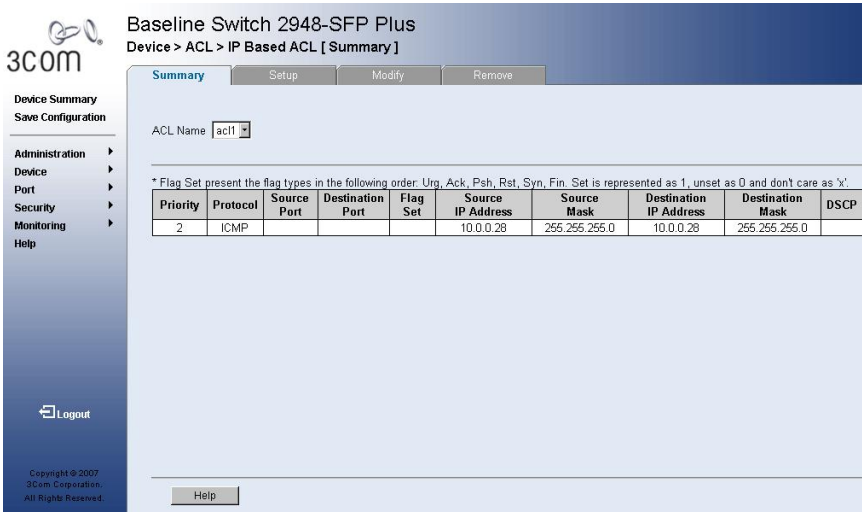
Viewing IP Based ACLs

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 31 IP Based ACL Summary Page



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

- **ACL Name** — Contains a list of the IP Based ACLs.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-65535, with 1 being the highest priority.
- **Protocol** — Indicates the protocol in the ACE to which the packet is matched.
- **Source Port** — Indicates the source port that is matched packets. Enabled only when TCP or UDP are selected in the Protocol list.

- **Destination Port** — Indicates the destination port that is matched 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 Address** — Matches the source IP address to which packets are addressed to the ACL.
- **Source Mask** — Indicates the source IP address mask.
- **Destination Address** — Matches the destination IP address to which packets are addressed to the ACL.
- **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** — 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 128 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 128.

Monitor users have no access to this page.

To configure IP Based Access Control Lists:

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

Figure 32 IP Based ACL Setup Page



Baseline Switch 2948-SFP Plus

Device > ACL > IP Based ACL [Setup]

SummarySetupModifyRemove

Selection ACL: acl1Create ACL

Add Rules to ACL:

Priority

ProtocolSelect from List ICMPProtocol ID

Source Port

Any

Destination Port

Any

TCP Flags

UrgSet

AckSet

PshSet

RstSet

SynSet

FinSet

Source IP Address

Wild Card Mask

Any

Dest. IP Address

Wild Card Mask

Any

Match DSCP

Match IP Precedence

Action

Permit

* 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'.

Priority	Protocol	Source Port	Destination Port	Flag Set	Source IP Address	Source Mask	Destination IP Address	Destination Mask	DSCP
2	ICMP				10.0.0.28	255.255.255.0	10.0.0.28	255.255.255.0	

Help

Device Summary

Save Configuration

Administration

Device

Port

Security

Monitoring

Help

Logout

Copyright © 2007

3Com Corporation.

All Rights Reserved.

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

- **Selection ACL** — Selects the ACL to be bound.
- **Create ACL** — Defines a new user-defined IP based ACL.

Add Rules to ACL

- **Priority** — Defines the ACL priority. ACLs are checked on the first fit basis. The ACL priority defines the ACL order in the ACL list.
- **Protocol** — Indicates the protocol in the ACE to which the packet is matched. The possible fields are:
 - *Select from List* — Selects a protocol on which ACE can be based.
 - *Protocol ID* — Select a protocol ID from a list on which ACE can be based.
- **Source Port** — Indicates 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** — Indicates 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 ACE, 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 no bit is important. A wildcard mask of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address is 149.36.184.198 and the wildcard mask is 0.0.0.255, 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 ACE, 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. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard mask of 0.0.0.0 indicates that all bits are important. For example, if the destination IP address 149.36.184.198 and the wildcard mask is 0.0.0.255, the first three bytes of the IP address are matched, while the last eight bits are ignored. For the destination 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 056.022.075.032 is invalid, but a wildcard mask of 56.22.75.32 is valid.

- **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.
 - **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.
 - **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.
- 2 Select an ACL from the ACL Name drop-down list.
- 3 Define the rule setup fields.
- 4 Click **Apply**. The Rule Setup settings are configured, and the device is updated.

Modifying IP Based ACLs

The *IP Based ACL Modify Page* allows the network administrator to modify IP Based ACLs settings.
Monitor users have no access to this page.

Figure 33 IP Based ACL Modify Page

3COM Baseline Switch 2948-SFP Plus
Device > ACL > IP Based ACL [Modify]

Summary Setup **Modify** Remove

Selection ACL **acl1**

* 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'.

Priority	Protocol	Source Port	Destination Port	Flag Set	Source IP Address	Source Mask	Destination IP Address	Destination Mask	DSCP
2	ICMP				10.0.0.28	255.255.255.0	10.0.0.28	255.255.255.0	

Modify Rule:

Priority:

Protocol: ☐ Select from List **ICMP** ☐ Protocol ID

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**

Help

Copyright © 2007 3Com Corporation. All Rights Reserved.

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

- **Selection ACL** — Selects the ACL to be modified.

Modify Rule

- **Priority** — Defines the ACL priority. ACLs are checked on the first fit basis. The ACL priority defines the ACL order in the ACL list.
- **Protocol** — Indicates the protocol in the ACE to which the packet is matched.
 - *Select from List* — Selects a protocol from a list on which ACE can be based.
 - *Protocol ID* — Select a protocol ID from a list on which ACE can be based.
- **Source Port** — Enables creating an ACL based on a specific protocol.
 - *Any* — Enables creating an ACL based on any protocol.

- **Destination Port** — Indicates the destination port that is matched packets. Enabled only when TCP or UDP are selected in the Protocol list.
- **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** — Matches the source IP address to which packets are addressed to the ACL.
 - *Wild Card Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that no bit is important. A mask of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address is 149.36.184.198 and the wildcard mask is 255.255.255.00, the first three bytes of the IP address are ignored, while the last eight bits are used.

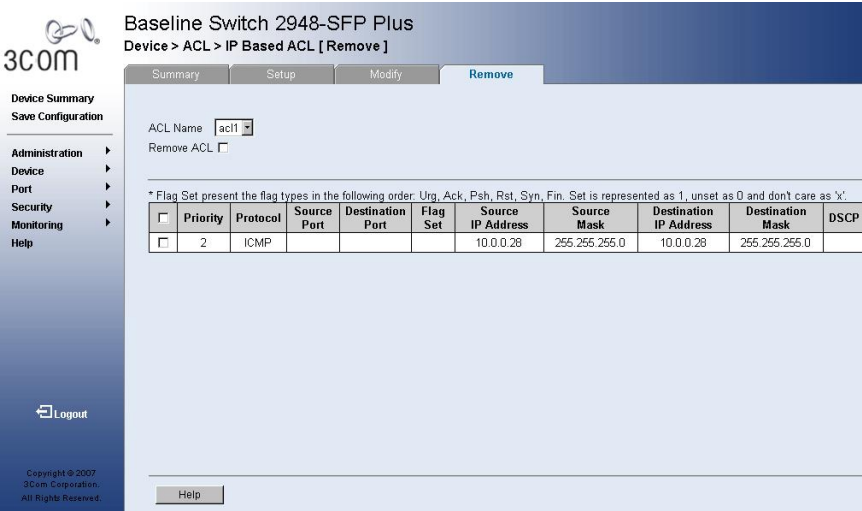
- **Destination IP Address** — Matches the destination IP address to which packets are addressed to the ACL.
 - *Wild Card Mask* — Indicates the destination IP Address wildcard mask. Wildcards are used to filter a destination IP Address. Masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard mask of 0.0.0.0 indicates that all bits are important.
For example, if the destination IP address 149.36.184.198 and the wildcard mask is 255.255.0.0, the first two bytes of the IP address are used, while the last two bytes are ignored.
- **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.
- **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.
- **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.

Removing IP Based ACLs

The *IP Based ACL Remove Page* allows the user to remove IP Based ACLs.
Monitor users have no access to this page.

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

Figure 34 IP Based ACL Remove Page



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

- **ACL Name** — Contains a list of the IP-based ACLs.
- **Remove ACL** — Removes an ACL. The possible field values are:
 - *Checked* — Removes the selected IP-based ACL.
 - *Unchecked* — Maintains the IP-based ACL.
- **Priority** — Indicates the ACL priority, which determines which ACL is matched to a packet on a first-match basis. The possible field values are 1-65535.
- **Protocol** — Indicates the protocol in the ACE to which the packet is matched.
- **Source Port** — Defines the TCP/UDP source port to which the ACL is matched.

- **Destination Port** — Defines the TCP/UDP destination port.
- **Flag Set** — Sets the indicated TCP flag matched to the packet.
- **Source Address** — Indicates the source IP address.
- **Source Mask** — Indicates the source IP address mask.
- **Destination 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** — 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.

2 Select an ACL to be removed.

3 Click **Apply**. The selected ACLs are deleted, and the device is updated.

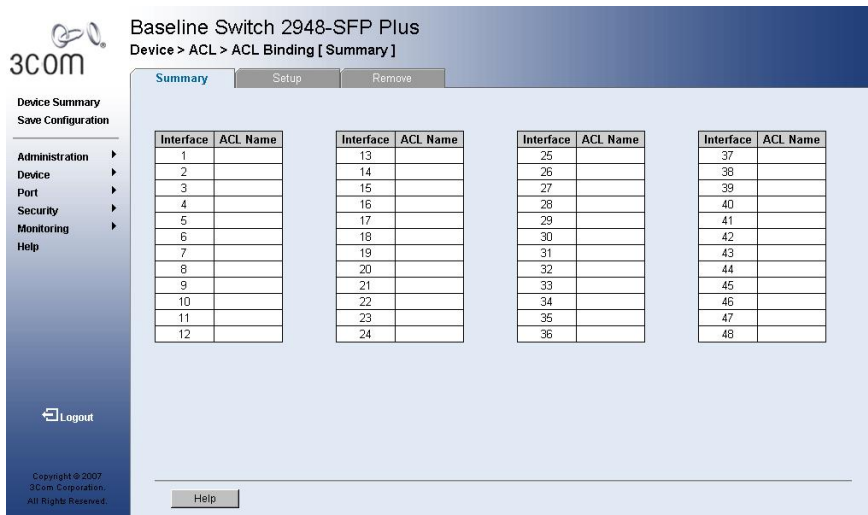
Viewing ACL Binding

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 35 ACL Binding Summary Page



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 ACL which is bound to a selected port.

Configuring ACL Binding

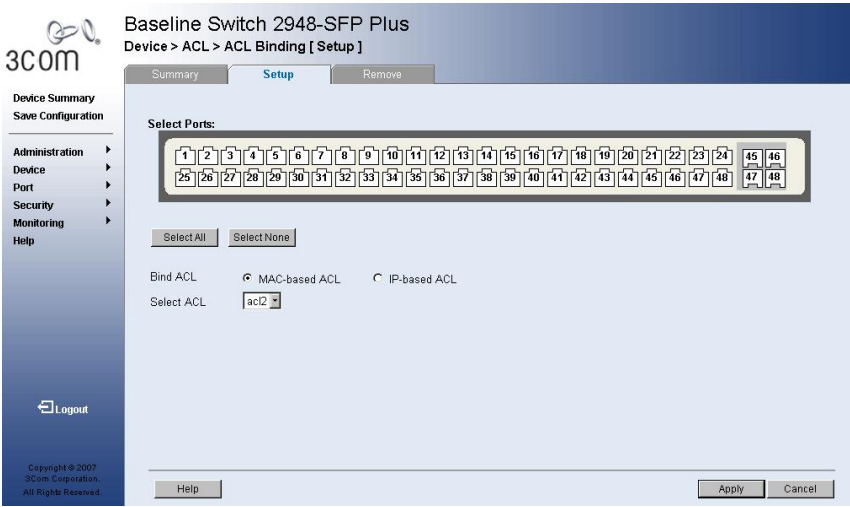
The *ACL Binding Setup Page* allows the network administrator to bind specific ports to MAC or IP Based ACLs.

The monitor user has no access to this page.

To define ACL Binding:

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

Figure 36 ACL Binding Setup Page



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

- **Select Port(s)** — Indicates the ports to be configured.
- **Select All** — Allows the user to assign the ACL to all ports.
- **Select None** — Removes the ports selected.
- **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** — Contains 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. *The monitor user has no access to this page.*

To remove ACL Binding:

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

Figure 37 ACL Binding Remove Page

Baseline Switch 2948-SFP Plus
Device > ACL > ACL Binding [Remove]

Summary Setup Remove

Device Summary
Save Configuration

Administration >
Device >
Port >
Security >
Monitoring >
Help

Logout

Copyright © 2007
3Com Corporation
All Rights Reserved

<input type="checkbox"/>	Interface	ACL Name
<input type="checkbox"/>	1	
<input type="checkbox"/>	2	
<input type="checkbox"/>	3	
<input type="checkbox"/>	4	
<input type="checkbox"/>	5	
<input type="checkbox"/>	6	
<input type="checkbox"/>	7	
<input type="checkbox"/>	8	
<input type="checkbox"/>	9	
<input type="checkbox"/>	10	
<input type="checkbox"/>	11	
<input type="checkbox"/>	12	

<input type="checkbox"/>	Interface	ACL Name
<input type="checkbox"/>	13	
<input type="checkbox"/>	14	
<input type="checkbox"/>	15	
<input type="checkbox"/>	16	
<input type="checkbox"/>	17	
<input type="checkbox"/>	18	
<input type="checkbox"/>	19	
<input type="checkbox"/>	20	
<input type="checkbox"/>	21	
<input type="checkbox"/>	22	
<input type="checkbox"/>	23	
<input type="checkbox"/>	24	

<input type="checkbox"/>	Interface	ACL Name
<input type="checkbox"/>	25	
<input type="checkbox"/>	26	
<input type="checkbox"/>	27	
<input type="checkbox"/>	28	
<input type="checkbox"/>	29	
<input type="checkbox"/>	30	
<input type="checkbox"/>	31	
<input type="checkbox"/>	32	
<input type="checkbox"/>	33	
<input type="checkbox"/>	34	
<input type="checkbox"/>	35	
<input type="checkbox"/>	36	

<input type="checkbox"/>	Interface	ACL Name
<input type="checkbox"/>	37	
<input type="checkbox"/>	38	
<input type="checkbox"/>	39	
<input type="checkbox"/>	40	
<input type="checkbox"/>	41	
<input type="checkbox"/>	42	
<input type="checkbox"/>	43	
<input type="checkbox"/>	44	
<input type="checkbox"/>	45	
<input type="checkbox"/>	46	
<input type="checkbox"/>	47	
<input type="checkbox"/>	48	

Help Remove Cancel

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

- **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 Select an ACL to be removed.

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

Viewing Broadcast Storm

Broadcast Storm 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.

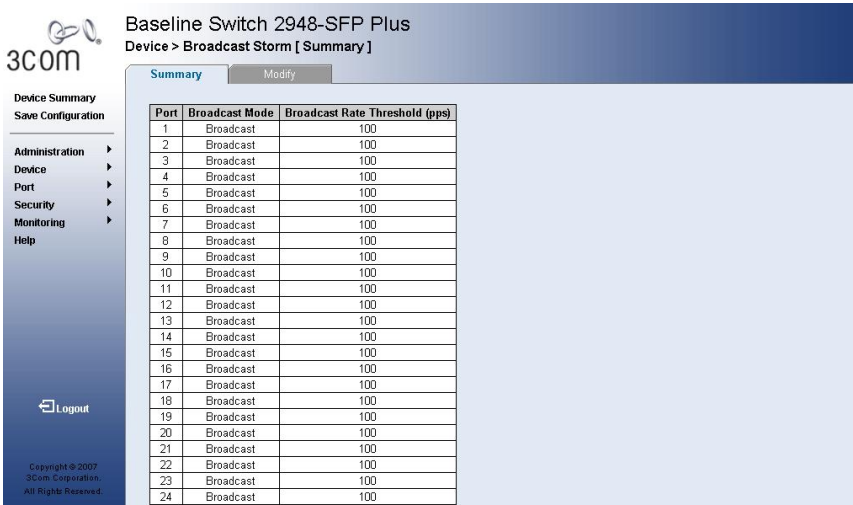
A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Broadcast Storm is enabled for all Gigabit ports by defining the packet type and the rate the packets are 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. Packet threshold is ignored if Broadcast Storm Control is Disabled.

To view Broadcast Storm Traffic:
1 Click **Device > Broadcast Storm > Summary**. The *Broadcast Storm Setup Page* opens.

Monitor users have no access to this page.

Figure 38 Broadcast Storm Summary Page



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

- **Port** — Indicates the selected port number.
- **Broadcast mode** —Indicates the packet types for the storming control. The possible mode values are:
 - *Disabled* — Disables storming control on the selected port.
 - *Broadcast* — Enables broadcast control on the selected port.
 - *Broadcast&Multicast* — Enables broadcast and multicast control the selected port.
- **Broadcast Rate Threshold** — Indicates the maximum rate (packets per second) at which Broadcast or Broadcast&Multicast packets are forwarded.

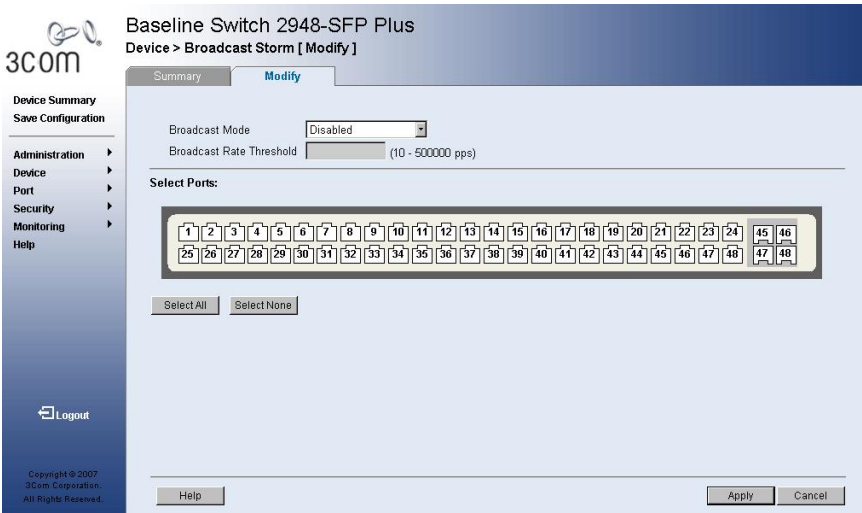
Modifying Broadcast Storm

The *Broadcast Storm Modify Page* allows the network administrator to modify Broadcast Storm settings.

Monitor users have no access to this page.

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

Figure 39 Broadcast Storm Modify Page



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

- **Broadcast Mode** — Indicates if forwarding Broadcast packet types is enabled on the interface.
 - *Disabled* — Disables broadcast control on the selected port.
 - *Broadcast* — Enables broadcast control on the selected port.
 - *Broadcast&Multicast* — Enables broadcast and multicast control on the selected port.

- **Broadcast Rate Threshold (10-500,000)** — Indicates the maximum rate (packets per second) at which Broadcast or Broadcast&Multicast packets are forwarded. The range is 10-500,000. The default value is 100.
 - **Select Port(s)** — Indicates the ports to be configured.
 - *Select All* — Allows the user to assign the Broadcast Mode to all ports.
 - *Select None* — Removes the ports selected.
- 2 Define the relevant fields.
- 3 Click **Apply** . Broadcast Storm is defined, and the device is updated.

5

GENERAL SYSTEM INFORMATION

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

- Viewing System Description
- Configuring System Name Information
- Configuring System Time

Viewing System Description

The *Device View Page* displays parameters for configuring general device information, including the system name, MAC Address, software and hardware versions, and more.

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

Figure 40 Device View Page

The screenshot shows the 3Com web interface for a Baseline Switch 2948-SFP Plus. The page title is "Baseline Switch 2948-SFP Plus" and the subtitle is "Device Summary [Device View]". The left sidebar contains a navigation menu with "Device Summary" and "Save Configuration" at the top, followed by "Administration", "Device", "Port", "Security", "Monitoring", and "Help". A "Logout" button is at the bottom of the sidebar. The main content area has a "Device View" tab selected. Above the information table is a grid of 48 numbered boxes, with box 16 highlighted in yellow and box 23 in green. Below the grid is a table titled "Device Summary Information" with the following data:

Device Summary Information	
Product Description:	3Com Baseline Switch 2948 Plus
System Name:	Baseline Switch 2948-SFP Plus
System Location:	
System Contact:	
Serial Number:	2JTTYWQ2B914C
Product 3C Number:	3CBL8G48
System Object ID:	1.3.6.1.4.1.43.1.8.62
MAC Address:	00:90:a1:2b:91:4c
System Up Time:	0 days, 0 hours, 10 minutes, 9 seconds
Software Version:	00.00.23
Boot Version:	00.00.11
Hardware Version:	1.0.1

At the bottom of the main content area, there is a "Poll Now" button and the text "The default polling interval is 60 sec". The footer of the page contains the copyright information: "Copyright © 2007 3Com Corporation. All Rights Reserved."

The *Device View Page* contains the following fields:

- **Product Description** — Displays the device model number and name. Not user-editable.
- **System Name** — Displays the user-defined device name. See “Configuring System Name Information” page 86.
- **System Location** — Displays the location where the system is currently running.
- **System Contact** — Displays the name of the contact person. See “Configuring System Name Information” page 86.
- **Serial Number** — Displays the device serial number. Not editable.
- **Product 3C Number** — Displays the 3Com device model number. Not editable.
- **System Object ID** — Displays the vendor’s authoritative identification of the network management subsystem contained in the entity. Not editable.
- **MAC Address** — Displays the device MAC address. Not editable.
- **System Up Time** — Displays the amount of time since the device was reset.
- **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** — This button immediately polls the switch ports for information including speed, use and status. The information is displayed by clicking the port icons at the top of the Device View tab. “Device Representation” page 25.

Configuring System Name Information

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 read-only permissions on this page.

To configure the System Name:

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

Figure 41 System Name Page

The screenshot displays the 3Com web interface for configuring a Baseline Switch 2948-SFP Plus. The breadcrumb trail indicates the path: Administration > System Name [System Name]. The left sidebar contains navigation links: Device Summary, Save Configuration, Administration (selected), Device, Port, Security, Monitoring, and Help. The main content area is titled 'System Name' and contains three input fields: System Name, System Location, and System Contact. At the bottom of the page, there are 'Help', 'Apply', and 'Cancel' buttons. The footer includes the 3Com logo, a 'Logout' button, and copyright information: Copyright © 2007 3Com Corporation. All Rights Reserved.

The *System Name Page* includes the following fields:

- **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.

2 Define the fields.

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

4 Be sure to save your configuration, or the changes will be lost when the switch is rebooted. To save the configuration, refer to “Saving the Configuration” on page 31.

Configuring System Time

The *System Time Setup Page* contains fields for defining system time parameters for the local hardware clock. Daylight Savings Time can be enabled on the device.

Monitor users have limited permissions on this page.

Country specific times need to be added manually.

To configure the System Time:

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

Figure 42 System Time Setup Page

The screenshot displays the 'System Time Setup' page for a 'Baseline Switch 2948-SFP Plus'. The page is divided into a left sidebar with navigation links (Device Summary, Save Configuration, Administration, Device, Port, Security, Monitoring, Help) and a main content area. The main area has a 'Setup' tab selected. It shows the 'Current Time' as 5:28:2007 7:41:48. Under 'Time Zone', 'GMT' is selected, and 'Daylight Saving' is unchecked. There are two radio button options: 'Use NTP Server' (selected) and 'Configure Date and Time Manually'. The NTP section includes fields for 'IP Address' (148.234.7.30) and 'Polling Interval (in mins)' (1440), with a 'Last Successful SNTP Connection' timestamp and an 'Update Now' button. The manual configuration section shows a date and time picker with fields for Mon, Day, Year, Hour, Min, and Sec, with values 5, 28, 2007, 7, 41, and 28 respectively. At the bottom, there are 'Help', 'Apply', and 'Cancel' buttons.

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

- **Current Time** — Displays the current time in Mon-Day-Year Hour:Min:Sec.
 - *Time Zone*: Selects the time zone.
- **Daylight Saving** — This check box enables and disables automatic Daylight Saving Time (DST) on the switch.
 - *USA* — 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
 - *European* — The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The European option applies to EU members, and other European countries using the EU standard.
- **Use NTP Server** —Use the Simple Network Time Protocol to get the time from the time server.
- **IP Address** — The IP address of the time server.
- **Polling Interval** — The time interval in minutes at which the switch synchronizes the time from the time server.
- **Last Successful NTP Connection** — Displays the last successful update from the time server.
- **Update Now** — The button to force the update from the time server right away. Click the “Apply” button before clicking this button when the IP address is changed to a new time server.
- **Configure Date and Time Manually** —Instead of using the time server, select this to configure the system time manually.

- 2 Define the Time Zone for the NTP server option.
- 3 Click the Daylight Saving Box to enable or disable automatic DST option.
- 4 Manually define the related fields for NTP server or local date and time.
- 5 Click **Apply**. The device is updated with the time settings.
- 6 Be sure to save your configuration, or the changes will be lost when the switch is rebooted. To save the configuration, refer to "Saving the Configuration" on page 31.

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

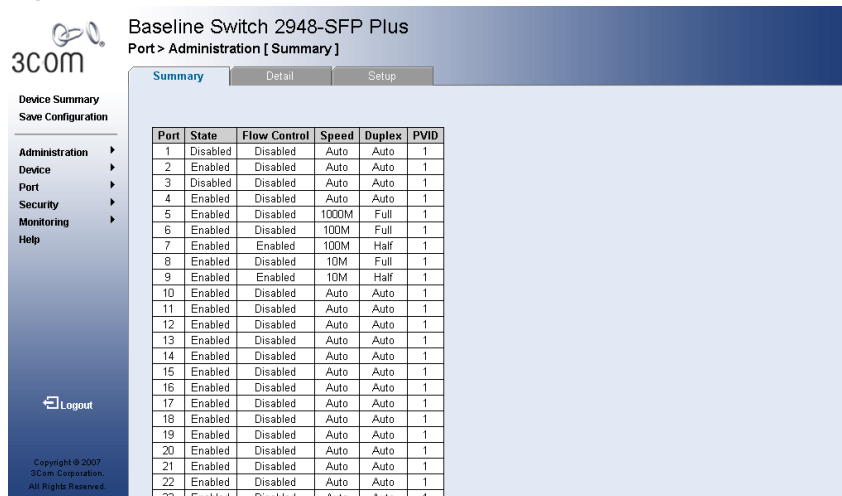
The Port Administration Summary Page permits the network manager to view the current port and LAG setting configuration. The *Port Administration Summary Page* also displays to which LAGs the port belongs. When configuring the port speed and port Duplex mode, please note the following:

- Setting the port speed to 10/100/1000 and the Duplex mode to Half = admin speed is = 10/100/1000 half and no advertisement.
- Setting the port speed to 10/100/1000 and the Duplex mode to Full = admin speed is = 10/100/1000 full and no advertisement.
- Setting the port speed to 10/100/1000 and the Duplex mode to Auto = admin speed is = Admin Advertisement = 10/100/1000 full and half.
- Setting the port speed to Auto and Duplex mode to Half = Admin Advertisement = 10+100+1000 half.
- Setting the port speed to Auto and Duplex mode to Full = Auto - Admin Advertisement = 10+100+1000 and Full.
- Setting the port speed to 10/100/1000 and the Duplex mode to Auto = Admin Advertisement = 10/100/1000 Full+Half.

To view Port Settings:

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

Figure 43 Port Administration Summary Page



Baseline Switch 2948-SFP Plus
Port > Administration [Summary]

Summary Detail Setup

Port	State	Flow Control	Speed	Duplex	PVID
1	Disabled	Disabled	Auto	Auto	1
2	Enabled	Disabled	Auto	Auto	1
3	Disabled	Disabled	Auto	Auto	1
4	Enabled	Disabled	Auto	Auto	1
5	Enabled	Disabled	1000M	Full	1
6	Enabled	Disabled	100M	Full	1
7	Enabled	Enabled	100M	Half	1
8	Enabled	Disabled	10M	Full	1
9	Enabled	Enabled	10M	Half	1
10	Enabled	Disabled	Auto	Auto	1
11	Enabled	Disabled	Auto	Auto	1
12	Enabled	Disabled	Auto	Auto	1
13	Enabled	Disabled	Auto	Auto	1
14	Enabled	Disabled	Auto	Auto	1
15	Enabled	Disabled	Auto	Auto	1
16	Enabled	Disabled	Auto	Auto	1
17	Enabled	Disabled	Auto	Auto	1
18	Enabled	Disabled	Auto	Auto	1
19	Enabled	Disabled	Auto	Auto	1
20	Enabled	Disabled	Auto	Auto	1
21	Enabled	Disabled	Auto	Auto	1
22	Enabled	Disabled	Auto	Auto	1
23	Enabled	Disabled	Auto	Auto	1
24	Enabled	Disabled	Auto	Auto	1

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

- **Port** — Indicates the selected port number.
- **Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
 - *Enabled* — Indicates the port is enabled.
 - *Disabled* — Indicates the port is 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. Port speeds can only be configured when auto-negotiation is disabled. 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 the port speed is configured to auto-negotiation.
- **Duplex** — Displays the port duplex mode. This field is configurable only when auto-negotiation is disabled, and the port speed is set to 10M or 100M or 1000M per second. 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* — Indicates the port duplex is configured to auto-negotiation.
- *PVID* — Displays the VLAN ID for the indicated port. The port will apply this VLAN ID to any untagged packet it receives

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.

To configure Port Settings:

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

Figure 44 Port Administration Setup Page

Baseline Switch 2948-SFP Plus
Port > Administration [Setup]

Summary Detail **Setup**

Port State Flow Control
Speed Duplex

Select Ports:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	45	46
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48		

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** — Defines the port state. The possible values are:
 - *No Change* — Retains the current port status.
 - *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.
 - *No Change* — Retains the current flow control status on port.

- **Speed** — Defines the configured rate for the port. The port speed determines what speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. 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** — Defines the port duplex mode. This field is configurable only when auto-negotiation is disabled. This field cannot be configured on LAGs. The possible field values are:
 - *Auto* — Use to automatically configure the port.
 - *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.
 - *No Change* — Retains the current port duplex mode.
 - *Select Ports* — Indicates the ports to be configured.
 - *Select All* — Allows the user to assign the settings to all ports.
 - *Select None* — Removes the ports selected.
- 2 Define the fields.
 - 3 Click **Apply**. The ports setting are applied, and the device is updated.

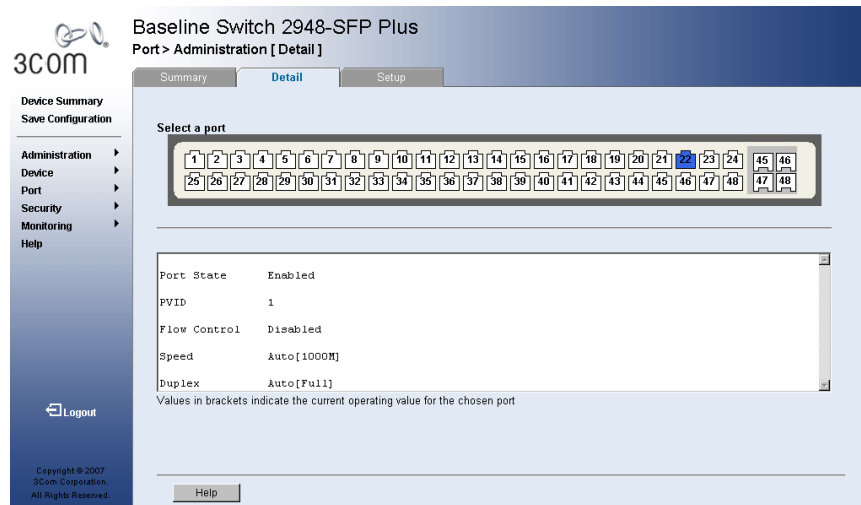
Viewing Port Details

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

To view Port Details:

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

Figure 45 Port Detail Page



The *Port Detail Page* contains the following fields:

- **Select a Port** — Displays the current port settings.
- **Port State** — Indicates the port state. The possible field values are:
 - *Enabled* — Enables the port.
 - *Disabled* — Disables the port.
- **PVID** — Indicates VLAN ID of this port for untagged packets.
- **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. Port speeds can only be configured when auto-negotiation is disabled. 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. The actual speed will show in brackets if the link is up.

The value in the bracket indicates the current operating speed.

- **Duplex** — Displays the port duplex mode. This field is configurable only when auto-negotiation is disabled. This field cannot be configured on LAGs. The possible field values are:
 - *Auto* — Use to automatically configure the port. The actual duplex will show in brackets if the link is up.
 - *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.
- 2 Select port to view the port detail.

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 LAG. A Link Aggregated Group (LAG) aggregates ports or VLANs into a single virtual port or VLAN. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. Ensure the following:

- All ports added to an existing LAG which are part of a tagged VLAN inherit the existing VLAN tags.
- Auto-negotiation mode is configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to eight LAGs, and eight ports in each LAG.

This section contains the following topics:

- Viewing Link Aggregation
- Configuring Link Aggregation
- Modifying Link Aggregation
- Removing Link Aggregation
- Viewing LACP
- Defining LACP Priority
- Defining LACP Port

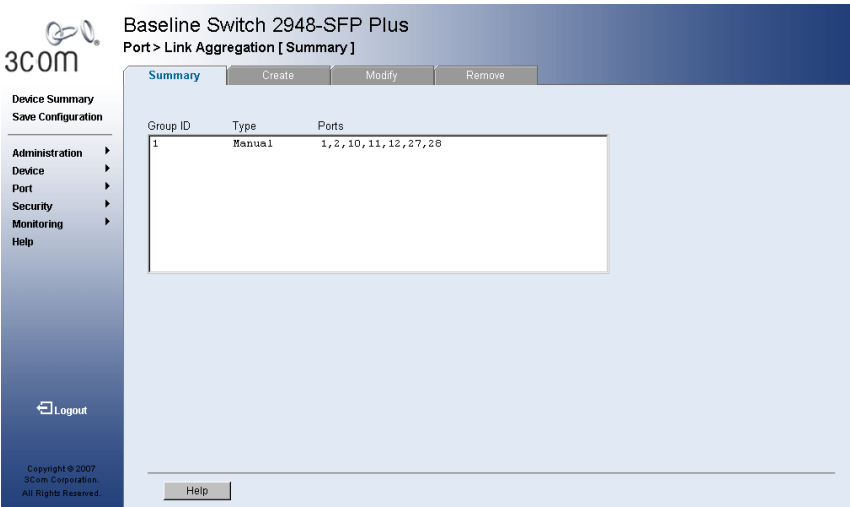
Viewing Link Aggregation

The *Link Aggregation Summary Page* displays port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

To view Link Aggregation:

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

Figure 46 Link Aggregation Summary Page



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

- **Group ID** — Displays the Link Aggregated Group ID.
- **Ports** — Displays the member ports included in the specified LAG.
- **Type** — Displays the type of link aggregation for the Group ID.
- **Manual** — A static link aggregation group created by network administrators.
- **LACP** — A link aggregation group created by LACP.

Configuring Link Aggregation

The *Link Aggregation Create Page* optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Monitor users have no access to this page.

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

Figure 47 Link Aggregation Create Page

Baseline Switch 2948-SFP Plus
Port > Link Aggregation [Create]

Summary Create Modify Remove

Enter Aggregation Group ID : (1-8)

Select ports for the new aggregation :

Selected Ports: ☒ Member of the aggregation being created. Deselected Ports: ☐ Not a member of any aggregation. ☐ Member of an existing aggregation or VLAN.

Summary

Group ID	Type	Member Ports
1	Manual	1, 2, 10, 11, 12, 27, 28

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

- **Enter aggregation Group ID** — Displays the group ID. The range is 1-8 groups.
- **Select ports for the new aggregation** — Displays the ports for which the link aggregation parameters are defined.
- **Blue** — Displays a member of the aggregation being created.
- **White** — Displays a non-existent member of any aggregation.
- **Grey** — Displays a member of an existing aggregation or VLAN.

Summary

- **Group ID** — Displays the Link Aggregated Group ID.
 - **Type** — Displays the type of link aggregation for the Group ID.
 - **Member Ports** — Displays the ports configured to the LAG.
- 2 Define the fields.
 - 3 Click **Apply**. The LAG configuration is defined, and the device is updated.

Modifying Link Aggregation

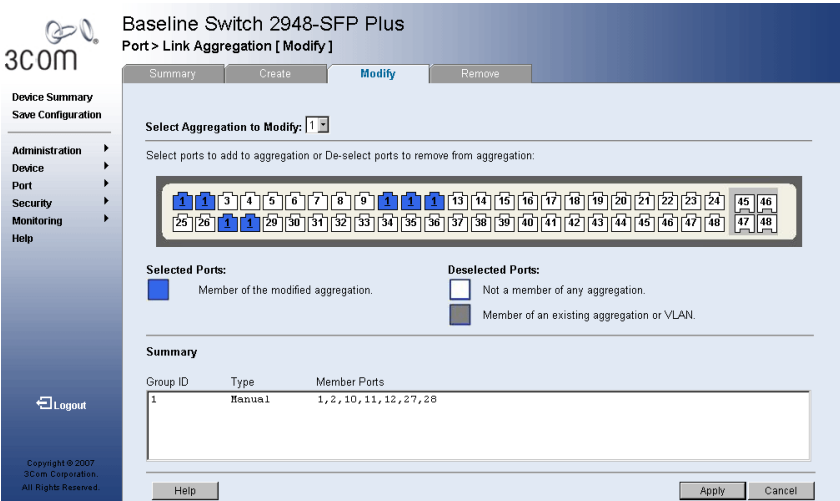
The *Link Aggregation Modify Page* optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

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 48 Link Aggregation Modify Page



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

- **Select Aggregation to Modify** — Selects the Link Aggregation Group ID to modify.
- **Selected Ports** — Allows the network manager to select ports to be added or removed from a current aggregation. The selected or deselected ports are color-coded as follows:
 - *Blue* — Displays a member of the modified aggregation.
 - *White* — Not a member of any aggregation.
 - *Grey* — Displays a member of an existing aggregation or VLAN.

Summary

- **Group ID** — Displays the Link Aggregated Group ID.
 - **Type** — Displays the type for link aggregation type the Group ID.
 - **Member Ports** — Displays the ports configured to the LAG.
- 2 Define the fields.
 - 3 Click **Apply**. Link Aggregation is configured, and the application is updated.

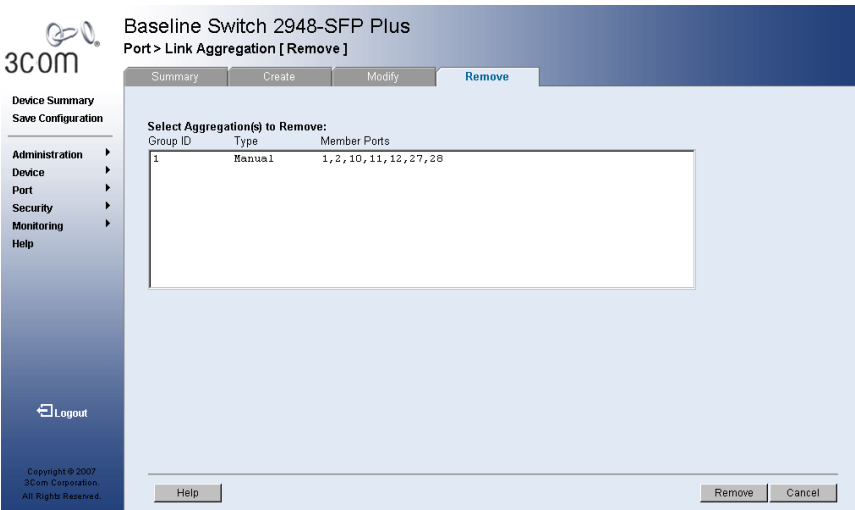
Removing Link Aggregation

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 49 Link Aggregation Remove Page



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

- **Select Aggregation(s) to Remove** — Displays the Link Aggregation table. Each row corresponds to a Link Aggregated Group ID. The fields in the table are:
 - *Group ID* — Displays the Link Aggregated Group ID.
 - *Type* — Displays the Link Aggregation type.
 - *Member Ports* — Displays the ports for which the link aggregation parameters are defined.
- 2 Select a group ID to be removed
- 3 Click **Remove**. The Link aggregation is removed, and the device is updated.

Viewing LACP

LAG ports can contain different media types if the ports are operating at the same speed. 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* contains fields for viewing LACP LAGs.

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

Figure 50 LACP Summary Page



Baseline Switch 2948-SFP Plus
Port > LACP [Summary]

Summary Setup Port Setup

Port	Status	Port Priority	State	Oper Key	Partner State	Partner Oper Key	Group ID
1	disabled	1001	N/A	N/A	N/A	N/A	N/A
2	disabled	1002	N/A	N/A	N/A	N/A	N/A
3	disabled	1003	N/A	N/A	N/A	N/A	N/A
4	disabled	1004	N/A	N/A	N/A	N/A	N/A
5	disabled	1005	N/A	N/A	N/A	N/A	N/A
6	disabled	1006	N/A	N/A	N/A	N/A	N/A
7	disabled	1007	N/A	N/A	N/A	N/A	N/A
8	disabled	1008	N/A	N/A	N/A	N/A	N/A
9	disabled	1009	N/A	N/A	N/A	N/A	N/A
10	disabled	1010	N/A	N/A	N/A	N/A	N/A
11	disabled	1011	N/A	N/A	N/A	N/A	N/A
12	disabled	1012	N/A	N/A	N/A	N/A	N/A
13	disabled	1013	N/A	N/A	N/A	N/A	N/A
14	disabled	1014	N/A	N/A	N/A	N/A	N/A
15	disabled	1015	N/A	N/A	N/A	N/A	N/A
16	disabled	1016	N/A	N/A	N/A	N/A	N/A
17	disabled	1017	N/A	N/A	N/A	N/A	N/A
18	disabled	1018	N/A	N/A	N/A	N/A	N/A
19	disabled	1019	N/A	N/A	N/A	N/A	N/A
20	disabled	1020	N/A	N/A	N/A	N/A	N/A
21	disabled	1021	N/A	N/A	N/A	N/A	N/A
22	disabled	1022	N/A	N/A	N/A	N/A	N/A
23	disabled	1023	N/A	N/A	N/A	N/A	N/A
24	disabled	1024	N/A	N/A	N/A	N/A	N/A

The *LACP Summary Page* contains the following fields:

- **Port** — Displays the port number.
- **Status** — Displays the administrative status of the port.
 - *Enabled* — LACP is enabled on the port
 - *Disabled* — LACP is disabled on the port
- **Port-Priority** — Displays the LACP priority value for the port. The field range is 0-65535.
- **State** — Displays inactive or active.
- **Oper Key** — Displays the operational key value assigned to the port by the switch.

- **Partner State** — Displays inactive or active
- **Partner Oper Key** — Displays the operational key value assigned to the port by the link partner.
- **Group ID** — Displays the group ID

Defining LACP Priority

LAG ports can contain different media types if the ports are operating at the same speed. 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 Setup Page* contains the field to configure the system priority.

- 1 Click **Port > LACP > Setup**. The *LACP Setup Page* opens.

Figure 51 LACP Setup Page

The screenshot shows the 'Baseline Switch 2948-SFP Plus' configuration page for 'Port > LACP [Port Setup]'. The interface has a left sidebar with navigation links: 'Device Summary', 'Save Configuration', 'Administration', 'Device', 'Port', 'Security', 'Monitoring', and 'Help'. The main content area has tabs for 'Summary', 'Setup', and 'Port Setup' (which is active). Under the 'Port Setup' tab, there are fields for 'Status' (set to 'Disabled') and 'Port Priority' (set to '0-65535'). Below these is a 'Select Ports:' section with a grid of 48 port selection buttons arranged in two rows of 24. The first row contains buttons numbered 1 through 24, and the second row contains buttons numbered 25 through 48. Below the grid are 'Select All' and 'Select None' buttons. At the bottom of the page are 'Help', 'Apply', and 'Cancel' buttons. The footer includes copyright information for 3Com Corporation, 2007.

The *LACP Setup Page* contains the following field:

- **System priority**— Specifies system priority value. The field range is 0-65535. The field default is 32767.
- 2 Define the fields.
 - 3 Click **Apply**. Link Aggregation is modified, and the application is updated.

Defining LACP Port

LAG ports can contain different media types if the ports are operating at the same speed. 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 Port Setup Page* contains fields for modifying LACP LAGs.

- 1 Click **Port > LACP > Port Setup**. The *LACP Port Setup Page* opens.

Figure 52 LACP Port Setup Page

Baseline Switch 2948-SFP Plus
Port > LACP [Port Setup]

Summary Setup **Port Setup**

Status:

Port Priority:

Select Ports:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

- **Status** — Displays the administrative LACP function. The possible field values are:
 - *Disabled* — Disables the LACP function on the selected ports.
 - *Enabled* — Enables the LACP function on the selected ports.
 - **Port Priority** — Displays the LACP priority value for the port. The field range is 0-65535.
 - **Select Ports** — Displays the port number to which timeout and priority values are assigned.
 - *Select All* — Allows the user to assign LACP status and port priority to all ports.
 - *Select None* — Removes the ports selected.
- 2 Define the fields.
 - 3 Click **Apply**. Link Aggregation is modified, and the application is updated.

8

CONFIGURING VLANS

This section contains the following topics:

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

VLAN Overview

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.



VLAN1 is the management VLAN. You can only manage the switch through a port that is an untagged member of VLAN1.

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 working at a protocol level 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. VLAN1 is the default VLAN. All ports are untagged members of VLAN1 by default. If any port becomes an untagged member of a different VLAN, then the port is removed from untagged membership of VLAN1. For example: If port 24 is made an untagged member of VLAN 5, the port will no longer be a member of VLAN1. However, if the port is made a tagged member of VLAN5, it still remains untagged in VLAN1.

A port can only be an untagged member of one VLAN. By default it is untagged member of VLAN1. If its untagged membership from another VLAN is removed, it will default to untagged membership in VLAN1.

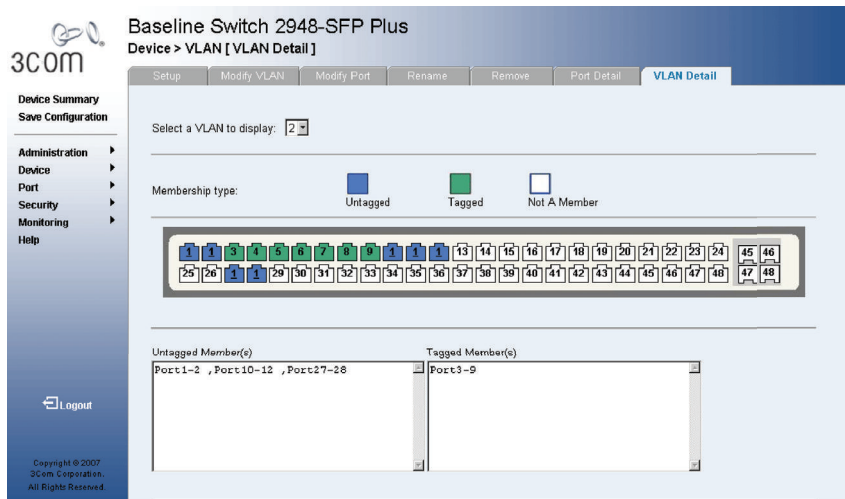
There is no restriction on tagged membership. A port can be a tagged member of any number of multiple VLANs.

Viewing VLAN Details

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

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

Figure 53 VLAN Detail Page



The *VLAN Detail Page* contains the following information:

- **Select a VLAN to display** — Selects a VLAN to be display.
- **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 packets are forwarded by the interface. The packets contain VLAN information.
- **Not a Member** — Indicates the interface is not a member of the VLAN

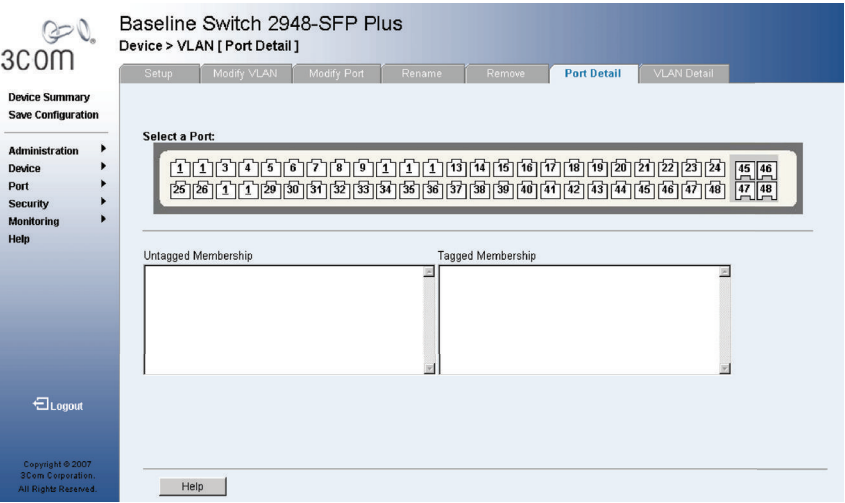
Viewing VLAN Port Details

The VLAN Port Detail Page provides displays VLAN configured ports.

To view VLAN Port details:

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

Figure 54 VLAN Port Detail Page



The VLAN Port Detail Page contains the following information:

- **Select Port** — Selects the port to be displayed.
- **Untagged membership** — Indicates the port is an untagged member of the VLAN.
- **Tagged membership** — Indicates the port is a tagged member of a VLAN. VLAN tagged packets are forwarded by the interface. The packets contain VLAN information.

Creating VLANs

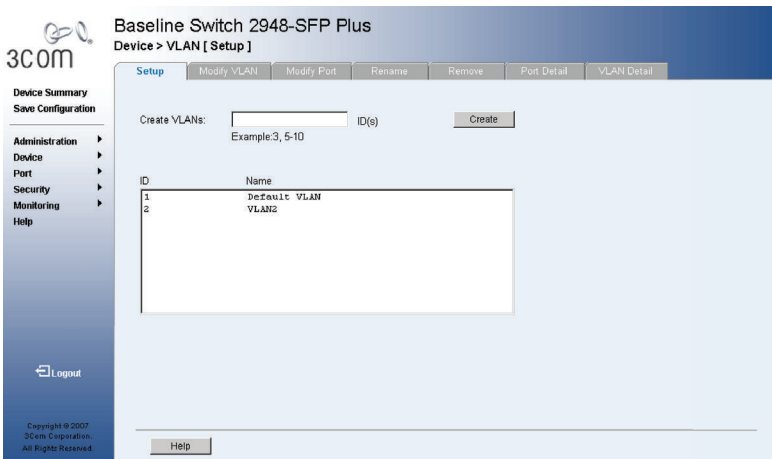
The *VLAN Setup Page* allows the network administrator to create user-defined VLANs. To view Voice VLAN Settings:

The monitor users have no access to this page.

To create VLANs:

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

Figure 55 VLAN Setup Page



The VLAN Setup Page contains the following fields:

Create

- **VLAN IDs** — Creates a VLAN ID.
 - **ID** — Displays the VLAN ID.
 - **Name** — Displays the user-defined VLAN name. Rename VLAN
- 2 Enter a VLAN Number.
 - 3 Click **Create**. The VLANs are configured, and the device is updated.

Rename the VLANS

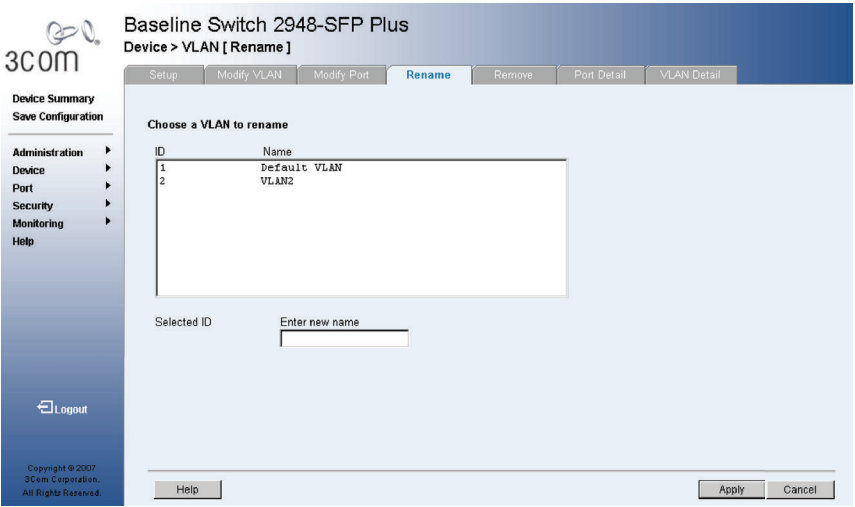
The *VLAN Rename Page* allows the network administrator to rename user-defined VLAN name.

The monitor users have no access to this page.

To rename VLANs:

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

Figure 56 VLAN Rename Page



The *VLAN Rename Page* contains the following fields:

- **Selected ID** — Displays the selected VLAN ID.
- **Enter new Name** — Renames the user-defined VLAN name.

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 **Rename**. The VLAN is renamed and the device is updated.

Modifying VLAN Settings

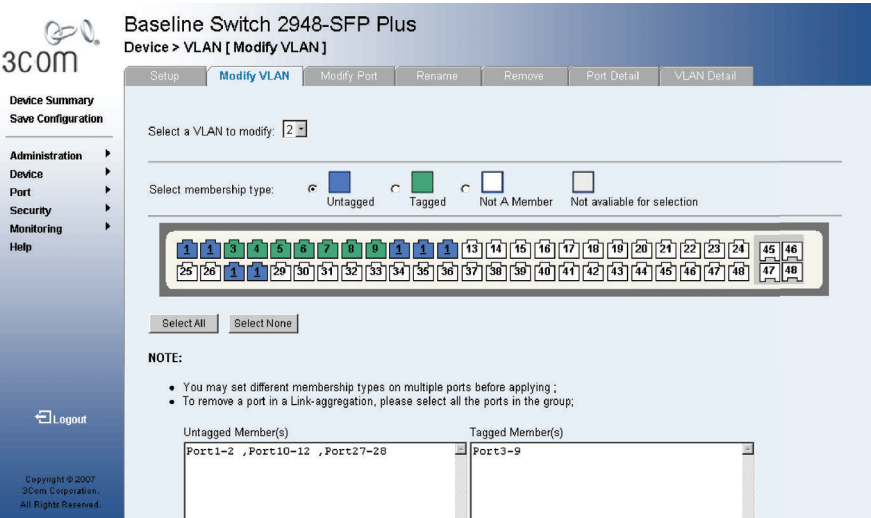
The *Modify VLAN Page* allows the network manager to change VLAN membership.

The monitor users have no access to this page.

To edit VLAN Settings:

- 1 Click **Device > VLAN > Modify VLAN**. The Modify VLAN Page opens.

Figure 57 Modify VLAN Page



The *Modify VLAN Page* contains the following fields:

- **Select a VLAN to Modify** — Select a VLAN name to be displayed.

- **Select 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 packets are forwarded by the interface.
 - **The packets 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 the user 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 port.
- 3 Select ports to be added to the selected VLAN.
- 4 Click **Apply**. The selected ports are added to the VLAN, and the device is updated.

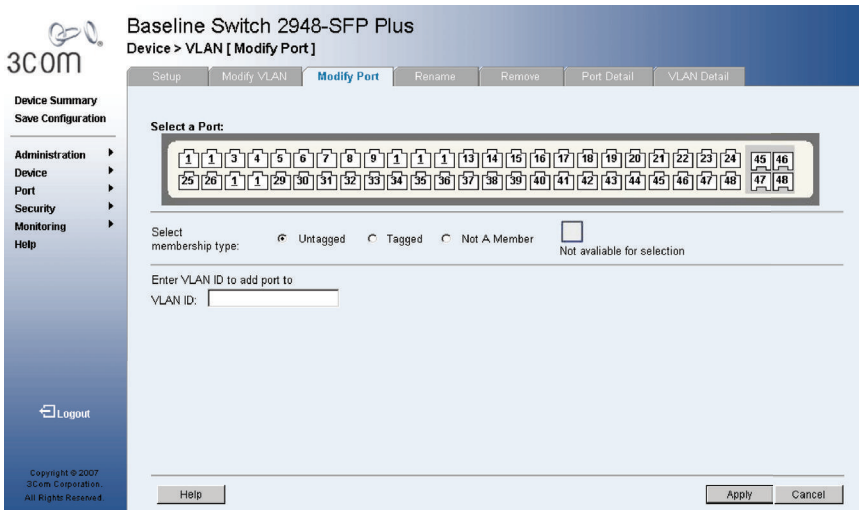
Modifying Port VLAN Settings

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

The monitor users have no access to this page.

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

Figure 58 Modify VLAN Port Page



The *Modify VLAN Port Page* contains the following fields:

- **Select a Port** — Selects a port to be modified.
- **Select Membership Type** — Displays the membership type for each VLAN. The possible field values are:
 - **Tagged** — Indicates the interface is a tagged member of a VLAN. VLAN tagged packets are forwarded by the interface. The packets contain VLAN information.
 - **Untagged** — Indicates the interface is an untagged member of the VLAN.
 - **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.
 - **VLAN ID** — Enter the VLAN ID to which the port is assigned.
 - **All Existing VLANs** — Change the selected port setting in the tagged membership of all the existing VLANs.
- 2 Select a port.
 - 3 Select Membership type.
 - 4 Enter VLAN ID to be assigned to the port.
 - 5 Click **Apply**. The VLANs are configured, and the device is updated.

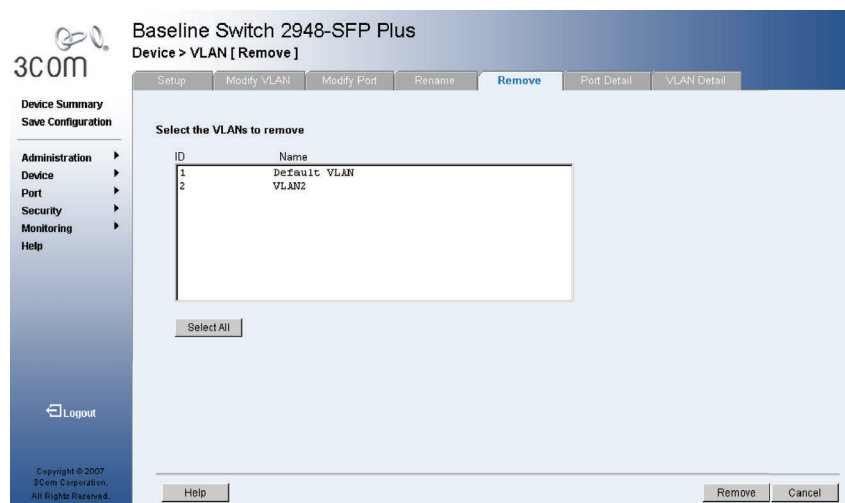
Removing VLANs

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

The monitor users have no access to this page.

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

Figure 59 VLAN Remove Page



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.
- 2 Select the VLAN ID 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
- Configuring Address Tables

Defining IP Addressing

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

The monitor user has no access to this page.

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

Figure 60 IP Setup Page

The screenshot displays the 'IP Setup' configuration page for a 'Baseline Switch 2948-SFP Plus'. The breadcrumb trail indicates the path: 'Administration > IP Setup [IP Setup]'. On the left, a navigation menu includes 'Device Summary', 'Save Configuration', and a list of categories: 'Administration', 'Device', 'Port', 'Security', 'Monitoring', and 'Help'. The 'IP Setup' section is active, showing two configuration methods: 'Static' (selected) and 'DHCP'. The 'Static' method description is 'User enters IP configuration'. Below this, there are input fields for 'IP Address' (169.254.145.76), 'Subnet Mask' (255.255.0.0), and 'Gateway'. At the bottom, there are 'Help', 'Apply', and 'Cancel' buttons. The footer contains copyright information: 'Copyright © 2007 3Com Corporation. All Rights Reserved.'

The *IP Setup Page* contains the following fields:

- **Configuration Method** — Indicates if the IP address has been configured statically or added dynamically. The possible field values are:
 - *Static* — Indicates that the IP Interface is configured by the user.
 - *DHCP* — Indicates that the IP Interface is dynamically created.
 - **IP Address** — Displays the currently configured IP address.
 - **Subnet Mask** — Displays the currently configured subnet mask.
 - **Default Gateway** — Displays the currently configured default gateway.
- 2 Select Static or DHCP mode.
 - 3 If Static has been selected, configure the IP Address, Subnet Mask and Default Gateway.
 - 4 Click **Apply**. The IP configuration is enabled, and the device is up dated.

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:

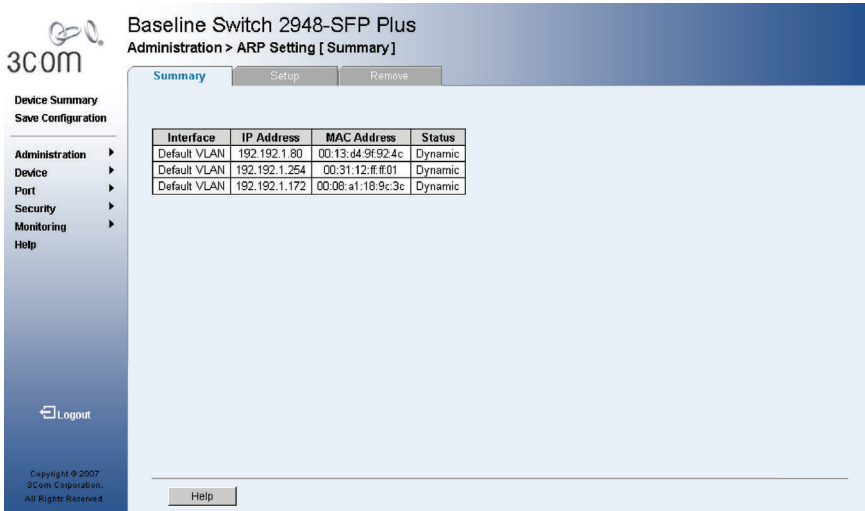
- Viewing ARP Settings
- Defining ARP Settings
- Removing ARP Entries

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 61 ARP Settings Summary Page



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

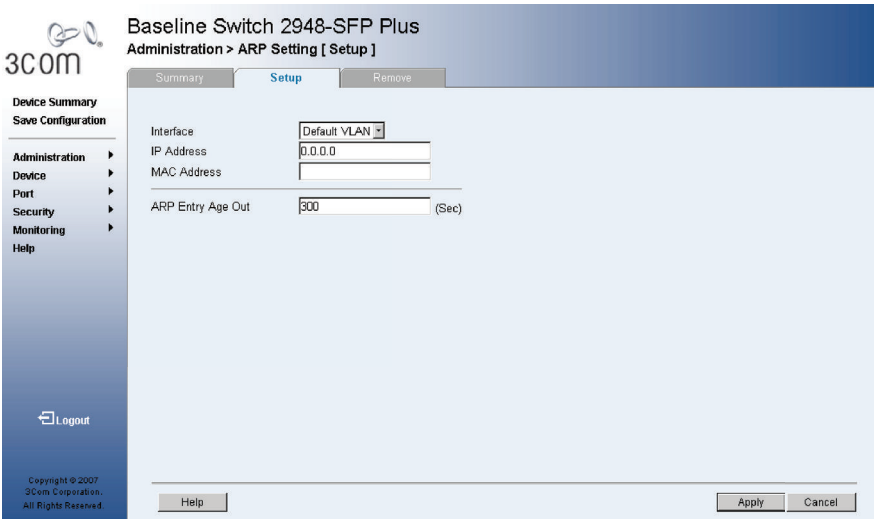
The *ARP Settings Setup Page* allows network managers to define ARP parameters for specific interfaces.

The 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 62 ARP Settings Setup Page



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

- **VLAN** — 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.
- **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 - 40000000. The default value is 300 seconds.

- 2 Define the fields.
- 3 Click **Apply**. The ARP parameters are defined, and the device is updated.

Removing ARP Entries

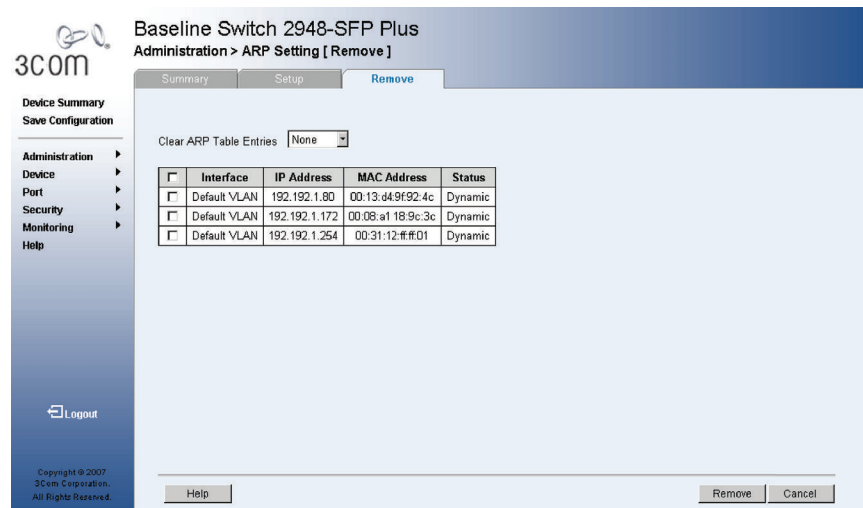
The *ARP Settings Remove Page* provides parameters for removing ARP entries from the ARP Table.

The monitor user has no access to this page.

To remove ARP entries:

- 1 Click **Administration > IP Addressing > ARP Settings > Remove**. The ARP Settings Remove Page opens.

Figure 63 ARP Settings Remove Page



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.

- **Remove** — Removes a specific ARP entry. The possible field values are:
 - *Checked* — Removes the selected ARP entries.
 - *Unchecked* — Maintains the current ARP entries.
 - **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 Select the Interface to be removed.
 - 3 Click **Remove**. The ARP interface is removed, and the device is updated.

Configuring Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address. MAC addresses are dynamically learned as packets from sources 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
- Adding Entries into Address Tables
- Defining Aging Time
- Removing Address Table Ports
- Removing Address Tables

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 Tables > Summary**. The *Address Table Summary Page* opens.

Figure 64 Address Table Summary Page

Baseline Switch 2948-SFP Plus
Monitoring > Address Table [Summary]

Summary Port Summary Add Setup Port Remove Remove

State
☒ All ☐ Static ☐ Dynamic

Summary

MAC Address	VLAN ID	State	Port Index	Aging Time
00:11:D8:27:8E:16	1	Dynamic	22	AGING
00:15:F2:A8:EA:CE	1	Dynamic	22	AGING
00:0C:29:2D:05:72	1	Dynamic	22	AGING
00:D0:B7:11:20:59	1	Dynamic	22	AGING
00:13:D4:52:40:A8	1	Dynamic	22	AGING
00:90:11:22:33:06	1	Dynamic	16	AGING
00:11:22:33:44:04	1	Dynamic	22	AGING
00:AD:80:14:83:55	1	Dynamic	22	AGING
00:0C:6E:F6:25:B8	1	Dynamic	22	AGING
00:02:44:7E:61:FA	1	Dynamic	22	AGING

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

Help

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

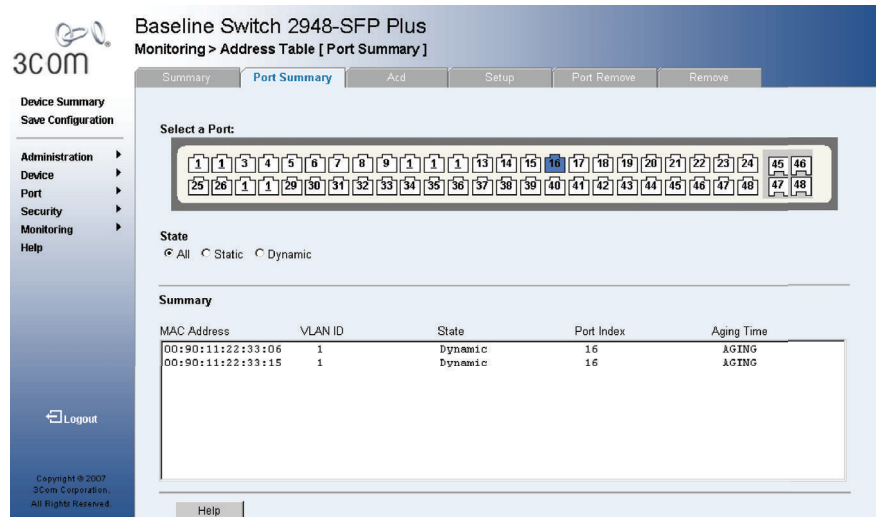
- **State** — Filters the list of MAC Addresses displayed according to the type of MAC Address configuration. Possible values are:
 - *All* — Displays all MAC Addresses.
 - *Static* — Displays the MAC Addresses that were entered by a user.
 - *Dynamic* — Displays the MAC Addresses that were detected by the switch.
- **MAC Address** — Displays the current MAC addresses listed in the MAC address table, filtered by the selected value of the State field.
- **VLAN ID** — Displays the VLAN ID attached to the MAC Address.
- **State** — Displays a table display based on the type of MAC address. Possible values are:
 - *Static* — Indicates the MAC address is statically configured.
 - *Dynamic* — Indicates the MAC address is dynamically configured.
- **Port Index** — Indicates the port through which the address was learned.
- **Aging Time** — Indicates that the MAC address is aged out or not.
- **NOAGED** — Indicates that the Address Table entry is not aged out.
- **AGING** — Indicates that the Address Table entry is aged out.

Viewing Port Summary Settings

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

- 1 Click **Monitoring > Address Tables > Port Summary**. The *Port Summary Page* opens.

Figure 65 Port Summary Page



The *Port Summary Page* contains the following fields:

- **Select a Port** — Displays the current port settings.
- **State** — Filters the list of MAC Addresses displayed according to the type of MAC Address configuration. Possible values are:
 - *All* — Displays all MAC Addresses assigned to the port.
 - *Static* — Displays static MAC Addresses assigned to the port.
 - *Dynamic* — Displays dynamic MAC Addresses assigned to the port.
- **MAC Address** — Displays MAC Addresses currently listed in the MAC Addresses table, filtered by the selected value of the State field.
- **VLAN ID** — Displays the VLAN ID attached to the MAC Address.

- **State** — Displays a port table display based on the type of address. Possible values are:
 - *Static* — Indicates the MAC Address is statically configured.
 - *Dynamic* — Indicates the MAC Address is dynamically configured.
- **Port Index** — Indicates Port Table number.
- **Aging Time** —Indicates that the MAC address is aged out or not.
- **NOAGED** — Indicates that the Address Table entry is not aged out.
- **AGING** — Indicates that the Address Table entry is aged out.

Adding Entries into Address Tables The *Address Table Add Page* allows the network manager to assign MAC addresses to ports with VLANs.

The monitor users have no access to this page.

To add Address Tables:

- 1 Click **Monitoring > Address Tables > Add**. The *Address Table Add Page* opens.

Figure 66 Address Table Add Page

3com Baseline Switch 2948-SFP Plus
Monitoring > Address Table [Add]

Summary Port Summary **Add** Setup Port Remove Remove

VLAN ID: 1

MAC Address: (For example:00:10:dc:28:a4:e9)

☐ No Aging

Select a Port:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Summary

MAC Address	VLAN ID	State	Port Index	Aging Time
00:11:D0:27:BE:16	1	Dynamic	22	AGING
00:15:F2:AB:EA:CE	1	Dynamic	22	AGING
00:0C:29:2D:85:72	1	Dynamic	22	AGING
00:D0:B7:11:20:59	1	Dynamic	22	AGING
00:13:D4:52:40:A8	1	Dynamic	22	AGING
00:90:11:22:33:06	1	Dynamic	16	AGING
00:11:22:33:44:04	1	Dynamic	22	AGING
00:A0:B0:14:E3:55	1	Dynamic	22	AGING
00:0C:6E:F6:25:B8	1	Dynamic	22	AGING
00:02:44:7E:61:FA	1	Dynamic	22	AGING

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

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

- **VLAN ID** — Assigns a VLAN ID to the user-defined MAC Address.
- **MAC Address** — Defines a MAC Address to be assigned to the specific port and VLAN ID.
- **No Aging** — Indicates that the MAC address assigned by the user is not aged out.
 - *Checked* — Indicates that the Address Table entry assigned by the user is not aged out.
 - *Unchecked* — Indicates that the Address Table entry assigned by the user is aged out.
- **Select a Port** — Select the port for which the MAC settings are defined.
- **MAC Address** — Displays the current MAC addresses listed in the MAC address table.
- **VLAN ID** — Displays the VLAN ID assigned to the user-defined MAC Address.
- **State** — Displays the current MAC Address state. Possible values are:
 - *Static* — Indicates that the Address Table entry assigned by
- **Port Index** — Indicates Port Table number.
- **Aging Time** — Indicates that the MAC address is aged out or not.
- **NOAGED** — Indicates that the Address Table entry is not aged out.
- **AGING** — Indicates that the Address Table entry is aged out.

2 Define the fields.

3 Click **Apply**. The MAC address is added to the address table, and the device is updated.

Defining Aging Time The *Address Table Setup Page* allows the network manager to define the Address Table Aging Time. The Aging Time is the amount of time the MAC Addresses remain in the Dynamic MAC Address Table before they are timed out if no traffic from the source is detected. The default value is 300 seconds.

The monitor users have no access to this page.

To define the Aging Time:

- 1 Click **Monitoring > Address Tables > Setup**. The *Address Table Setup Page* opens.

Figure 67 Address Table Setup Page

The screenshot displays the web management interface for a 3Com Baseline Switch 2948-SFP Plus. The breadcrumb navigation at the top indicates the path: Monitoring > Address Table [Setup]. The main content area features a tabbed interface with 'Setup' selected. Within the 'Setup' tab, there is a single configuration field labeled 'Aging time:' with a text input box containing the value '300'. To the right of the input box, a label specifies the unit and range: 'seconds (10-1000000, default=300)'. On the left side of the interface, a vertical sidebar contains a 'Device Summary' section with a 'Save Configuration' link, and a list of navigation links: Administration, Device, Port, Security, Monitoring, and Help. At the bottom of the sidebar is a 'Logout' button. The footer of the page includes copyright information for 2007 and a 'Help' button. The main content area has 'Apply' and 'Cancel' buttons at the bottom right.

The *Address Table Setup Page* contains the following field:

- **Aging Time** — Specifies the amount of time the MAC Address remains in the Dynamic MAC Address table before it is timed out if no traffic from the source is detected. The default value is 300 seconds.
- 2 Enter the desired aging time.
 - 3 Click **Apply**. The MAC address table configuration is enabled, and the device is updated.

Removing Address Table Ports

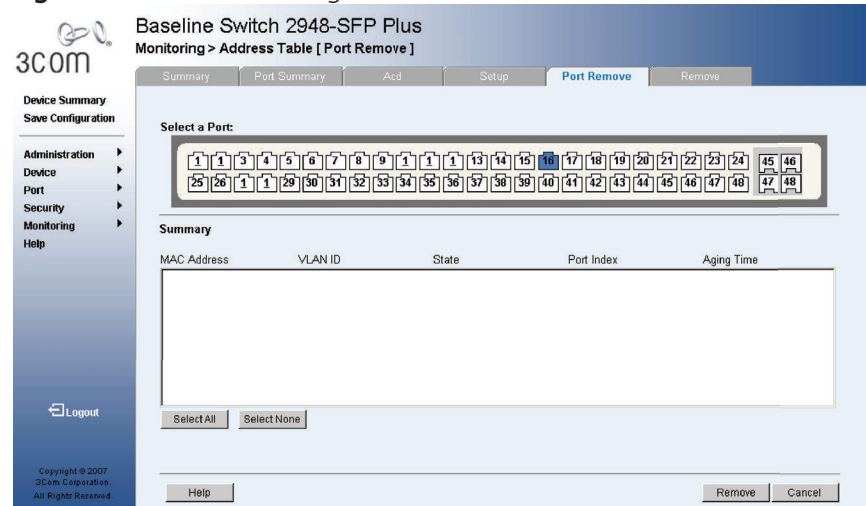
The *Port Remove Page* allows the network manager to remove ports from the address tables.

The monitor users have no access to this page.

To remove ports:

- 1 Click **Monitoring > Address Tables > Port Remove**. The Port Remove Page opens.

Figure 68 Port Remove Page



The *Port Remove Page* contains the following fields:

- **Select a Port** — Displays the current port settings.
- **MAC Address** — Displays the current MAC addresses listed in the MAC address table.
- **VLAN ID** — Displays the VLAN ID attached to the MAC Address.
- **State** — Displays the MAC address configuration method. Possible values are:
 - *Static* — Indicates the MAC address is statically configured.
 - *Dynamic* — Indicates the MAC address is dynamically configured.
- **Port Index** — Indicates Port Table number.

- **Aging Time** —Indicates that the MAC address is aged out or not.
 - **NOAGED** — Indicates that the Address Table entry is not aged out.
 - **AGING** — Indicates that the Address Table entry is aged out.
- 2 Select the port(s) to display MAC address on the table.
 3. Select the MAC addresses to remove.
 - 4 Click **Remove**. The selected MAC addresses are removed from the MAC address table, and the device is updated.

Remove address Table

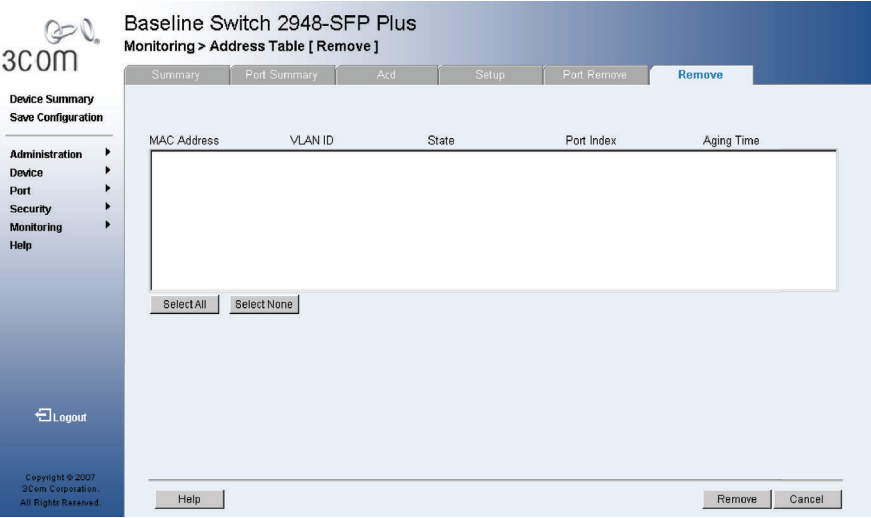
The *Address Table Remove Page* allows the network manager to remove current MAC addresses from the Address Table.

The monitor users have no access to this page.

To remove Address Tables:

- 1 Click **Monitoring > Address Table > Remove**. The *Address Table Remove Page* opens.

Figure 69 Address Table Remove Page



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

- **MAC Address** — Displays the current MAC addresses listed in the MAC address table.
 - **VLAN ID** — Displays the VLAN ID attached to the MAC Address.
 - **State** — Displays the MAC address configuration method. Possible values are:
 - *Static* — Indicates the MAC address is statically configured.
 - *Dynamic* — Indicates the MAC address is dynamically configured.
 - **Port Index** — Indicates Port Table number.
 - **Aging Time** — Indicates that the MAC address is aged out or not.
 - **NOAGED** — Indicates that the Address Table entry is not aged out.
 - **AGING** — Indicates that the Address Table entry is aged out.
 - **Select All** — Allows the user to select all table entries to remove
 - **Select None** — Removes the table entries selected.
- 2 Select the MAC addresses to remove.
 - 3 Click **Remove**. The selected MAC addresses are removed from the MAC address table, and the device is updated.

10

CONFIGURING IGMP SNOOPING & QUERY

Introduction

This section contains information for configuring IGMP Snooping & 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.
- Which routing protocols are forwarding packets and Multicast traffic.

When IGMP Snooping is enabled and IGMP Query globally, the device issues IGMP query.

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.

This section contains the following topic:

- Defining IGMP Snooping & Query

Defining IGMP Snooping & Query

The *IGMP Snooping & Query Setup Page* allows network managers to define GMP Snooping & Query parameters.

The monitor users have read-only access to this page.

- 1 Click **Device > IGMP Snooping & Query > Setup**. The *IGMP Snooping & Query Setup Page* opens.

Figure 70 IGMP Snooping & Query Setup Page

Baseline Switch 2948-SFP Plus
Device > IGMP Snooping & Query [Setup]

Setup

IGMP Snooping Status: Disabled
IGMP Query Status: Disabled

Select VLAN ID: 1
IGMP Snooping Status: Disabled
IGMP Query Status: Disabled

VLAN	Snooping Status	Query Status
1	Disabled	Disabled
2	Disabled	Disabled

Help Apply Cancel

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

- **IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the device. The possible field values are:
 - *Disabled* — Indicates that IGMP Snooping is Disabled on the device. This is the default value.
 - *Enabled* — Indicates that IGMP Snooping is enabled on the device.
- **IGMP Query Status** — Indicates if 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.
- **Select VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:

- *Disabled* — Disables IGMP Snooping on the VLAN. This is the default value.
 - *Enabled* — Enables IGMP Snooping on the VLAN.
 - **IGMP Query Status** — Indicates if 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.
- 2 Select Enabled IGMP Snooping.
 - 3 Define the fields.
 - 4 Click **Apply**. IGMP settings are applied, and the device is updated

11

CONFIGURING SPANNING TREE

This section contains information for configuring STP. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP 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 reducing network efficiency.

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

The device supports the following STP versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops.

- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops. While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

This section contains the following topics:

- Viewing Spanning Tree
- Defining Spanning Tree
- Modifying 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 71 Spanning Tree Summary Page

Baseline Switch 2948-SFP Plus
Device > Spanning Tree [Summary]

Summary Setup Port Setup

Port	Status	Path Cost	Edge Port	State	Link Type	Port Priority
1	Enabled	200000	Disabled	Discarding	Shared	128
2	Enabled	200000	Disabled	Discarding	Shared	128
3	Enabled	200000	Disabled	Discarding	Shared	128
4	Enabled	200000	Disabled	Discarding	Shared	128
5	Enabled	200000	Disabled	Discarding	Shared	128
6	Enabled	200000	Disabled	Discarding	Shared	128
7	Enabled	200000	Disabled	Discarding	Shared	128
8	Enabled	200000	Disabled	Discarding	Shared	128
9	Enabled	200000	Disabled	Discarding	Shared	128
10	Enabled	200000	Disabled	Discarding	Shared	128
11	Enabled	200000	Disabled	Discarding	Shared	128
12	Enabled	200000	Disabled	Discarding	Shared	128
13	Enabled	200000	Disabled	Discarding	Shared	128
14	Enabled	200000	Disabled	Discarding	Shared	128
15	Enabled	200000	Disabled	Discarding	Shared	128
16	Enabled	20000	Disabled	Forwarding	Point to Point	128
17	Enabled	200000	Disabled	Discarding	Shared	128
18	Enabled	200000	Disabled	Discarding	Shared	128
19	Enabled	200000	Disabled	Discarding	Shared	128
20	Enabled	200000	Disabled	Discarding	Shared	128
21	Enabled	200000	Disabled	Discarding	Shared	128
22	Enabled	20000	Disabled	Forwarding	Point to Point	128
23	Enabled	200000	Disabled	Discarding	Shared	128
24	Enabled	200000	Disabled	Discarding	Shared	128

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

- **Port** — The interface for which the information is displayed.
- **Status** — Indicates if STP or RSTP is enabled on the port. The possible field values are:
 - *Enabled* — Indicates that STP or RSTP is enabled on the port.
 - *Disabled* — Indicates that neither STP nor RSTP is enabled on the port.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is re-routed.

- **Edge Port** — Indicates if Edge Port is enabled on the port. If Edge Port is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Edge Port optimizes the STP protocol convergence. STP convergence takes 30 seconds and is not dependent on the number of switches in the network. However, an edge port that receives a BPDU immediately loses edge port status and becomes a normal spanning tree port. The possible field values are:
 - *Enabled* — Indicates that Edge Port is enabled on the port
 - *Disabled* — Indicates Edge Port is Disabled on the port.
- **State** — Displays the current STP state of a port. If enabled, the port state determines what action is taken on traffic. Possible port states are:
 - *Disabled* — Indicates that STP is currently Disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *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** — Displays the link type of the port. A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port by default. The possible field values are:
 - Point to point — Indicates that a point-to-point link is established on the port.
 - Shared — Indicates that a shared link is established on the port.

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

Defining Spanning Tree

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

The monitor user has no access to this page.

To configure Spanning Tree Setup:

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

Figure 72 Spanning Tree Setup Page

The screenshot displays the 'Spanning Tree Setup' page for a 'Baseline Switch 2948-SFP Plus'. The page has a sidebar with navigation links: Administration, Device, Port, Security, Monitoring, and Help. The main content area is titled 'Device > Spanning Tree [Setup]' and contains a table of configuration parameters. The 'Status' is set to 'Enabled'. The 'Priority' is '32768' with a note '(0-61440), in steps of 4096'. The 'STP Version' is 'RSTP'. The 'Hello Time' is '2' seconds '(1-10 seconds)'. The 'Forwarding Delay' is '15' seconds '(4-30 seconds)'. The 'Max Aging Time' is '20' seconds '(6-40 seconds)'. At the bottom, there are 'Help', 'Apply', and 'Cancel' buttons.

Parameter	Value	Range/Note
Status	Enabled	
Priority	32768	(0-61440), in steps of 4096
STP Version	RSTP	
Hello Time	2	(1-10 seconds)
Forwarding Delay	15	(4-30 seconds)
Max Aging Time	20	(6-40 seconds)

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

- **Status** — Indicates whether STP or RSTP is enabled on the device. The possible field values are:
 - *Enabled* — Enables STP or RSTP on the device.
 - *Disabled* — Disables STP and RSTP on the device.

-
- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, 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 port priority value is provided in increments of 4096.
 - **STP Version** — Specifies the STP version to run on the device. The possible field values are:
 - *STP* — Specifies STP to run on the device
 - *RSTP* — Specifies RSTP to run 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.
 - **Forward 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 Age** — 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 Maximum Age Time is 20 seconds.
- 2 Define the fields.
 - 3 Click **Apply**. STP settings are applied, and the device is updated.

Modifying Spanning Tree

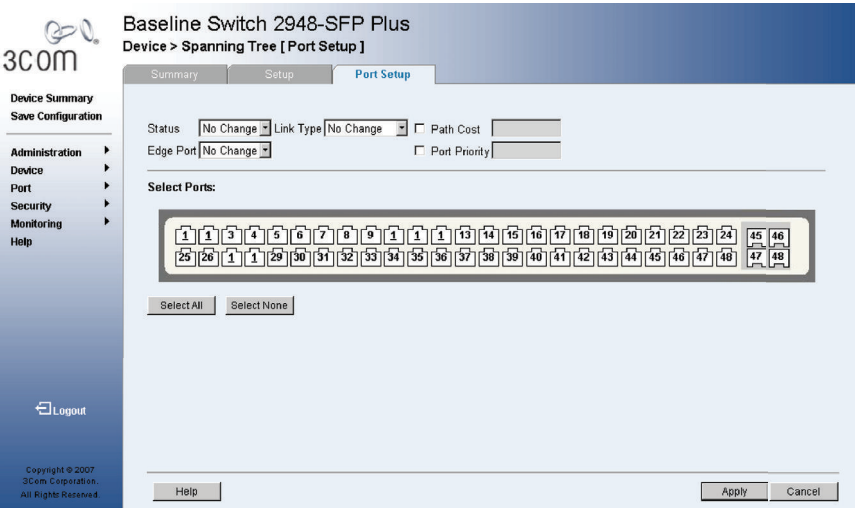
The *Spanning Tree Port Setup Page* contains information for modifying Spanning Tree parameters.

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 73 Spanning Tree Port Setup Page



The Spanning Tree Port Setup Page contains the following fields:

- **Status** — Specifies if STP is enabled on the port. The possible field values are:
 - *Enabled* — Specifies that STP is enabled on the port.
 - *Disabled* — Specifies that STP is disabled on the port.
 - *No Change* — Maintains the current STP settings. This is the default value.
- **Edge Port** — Specifies if Edge Port is enabled on the port. If Edge Port is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Edge Port optimizes the STP protocol convergence. STP convergence takes 30 seconds and is not dependent on the number of switches in the network. However, an edge port that receives a BPDU immediately loses edge port status and becomes a normal spanning tree port. The possible field values are:

- *Enabled* —Specifies the Edge Port is enabled on the port.
 - *Disabled* —Specifies the Edge Port is disabled on the port.
 - *No Change* —Maintains the current the Edge Port settings. This is the default value.
 - **Link Type** — Specifies the RSTP link type. The possible field values are:
 - *Point to Point* —Enables the device to establish a Point-to-Point link on the port. Ports set to Full Duplex modes are considered Point-to-Point port links.
 - *Shared* — Enables the device to establish a shared link on the port.
 - *Auto* — Enables the device to establish automatically a Point-to-Point link.
 - **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is re-routed. The field range is 1-200,000,000.
 - **Priority** — 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.
 - **Select Port(s)** — Indicates the ports to be defined.
 - *Select All* — Allows the user to assign the STP settings to all ports.
 - *Select None* — Removes the ports selected.
- 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:

- Defining SNMP Communities
- Removing SNMP Communities
- Defining SNMP Traps
- Removing SNMP Traps

Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Communities Setup Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

Monitor users have no access to this page.

To define SNMP communities:

- 1 Click **Administration > SNMP > Communities > Setup**. The *SNMP Communities Setup Page* opens.

Figure 74 SNMP Communities Setup Page

The screenshot shows the 'SNMP Communities Setup Page' for a 'Baseline Switch 2948-SFP Plus'. The page has a left sidebar with navigation links: Device Summary, Save Configuration, Administration, Device, Port, Security, Monitoring, and Help. The main content area has a title bar with 'Setup' and 'Remove' buttons. Below the title bar, there are several configuration sections:

- SNMP Status:** A dropdown menu set to 'Enable'.
- Insert New Community:** A checkbox that is checked, followed by 'SNMP Management' options: 'Management Station' (radio button) and 'Open Access' (radio button).
- Community String:** A section with 'Standard' (radio button) and 'User Defined' (radio button) options. The 'Standard' option is selected, and the 'Community String' field contains 'public'. Below this, the 'Access Mode' is set to 'Read Only'.
- Buttons:** 'Apply' and 'Cancel' buttons are located at the bottom right of the configuration section.
- Table:** A table with three columns: 'Management Station', 'Community String', and 'Access Mode'. It contains one row with the values 'All', 'Private', and 'Read Write'.
- Footer:** A 'Help' button is located at the bottom left of the page.

The *SNMP Communities Setup Page* contains the following fields:

- **SNMP Status** — Defines SNMP on the device. The possible field values are:
 - *Enabled* — Enables SNMP on the device.
 - *Disabled* — Disables SNMP on the device.
- **Insert New Community** — Adds a SNMP community string.

SNMP Management

- **Management Station** — Displays the management station IP address for which the SNMP community is defined.
- **Open Access** — Provides SNMP access to all the stations.

Community String

- **Standard** — Displays pre-defined community strings. The possible field values are:
 - *public* — Displays the pre-defined public community string name.
 - *private* — Displays the pre-defined private community string name.
 - **User Defined** — Defines a user-defined community string name.
 - **Access Mode** — Defines the access rights of the community. The possible field values are:
 - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
 - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
- 2 Define the relevant fields.
 - 3 Click **Apply**. The SNMP Communities are defined, and the device is updated.

Removing SNMP Communities

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

Monitor users have no access to this page.

To remove SNMP communities:

- 1 Click **Administration > SNMP > Communities > Remove**. The *SNMP Communities Remove Page* opens.

Figure 75 SNMP Communities Remove Page

Baseline Switch 2948-SFP Plus
Administration > SNMP > Communities [Remove]

Setup Remove

<input type="checkbox"/>	Management Station	Community String	Access Mode
<input type="checkbox"/>	All	Private	Read Write

Help Remove Cancel

The *SNMP Communities Remove Page* contains the following fields:

- **Remove** — Removes a community. The possible field values are:
 - *Checked* — Removes the selected SNMP community.
 - *Unchecked* — Maintains the SNMP communities.
- **Management Station** — 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.

- Access Mode — Displays the access rights of the community. The possible field values are:
 - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
 - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
- 2 Select the SNMP Community to be removed.
- 3 Click **Remove**. The SNMP Community is removed, and the device is updated.

Defining SNMP Traps

The *SNMP Traps Setup Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent.

Monitor users have no access to this page.

To define SNMP traps:

- 1 Click **Administration > SNMP > Traps**. The *SNMP Traps Setup Page* opens.

Figure 76 SNMP Traps Setup Page

3Com Baseline Switch 2948-SFP Plus
Administration > SNMP > Traps [Setup]

Setup Remove

Recipient IP Address
Community String
Trap Version

Apply Cancel

Recipient IP	Trap	Community String
10.0.0.29	SNMPv1	trap

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

Help

The *SNMP Traps Setup Page* contains the following fields:

- **Recipients IP Address** — Defines the IP address to which the traps are sent.
 - **Community String** — Defines the community string of the trap manager.
 - **Trap Version** — Defines the trap type. The possible field values are:
 - *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
 - *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
- 2 Define the relevant fields.
 - 3 Click **Apply**. The SNMP Traps are defined, and the device is updated.

Removing SNMP Traps

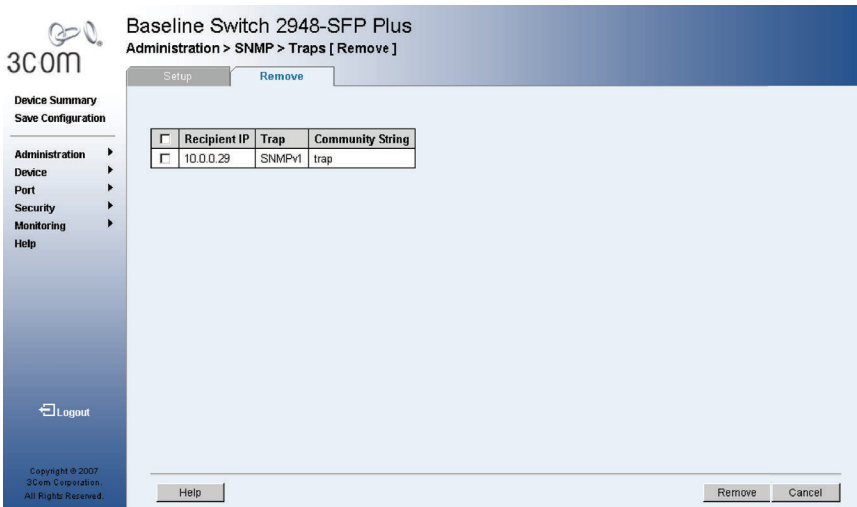
The *SNMP Traps Remove Page* allows the network manager to remove SNMP Traps.

Monitor users have no access to this page.

To remove SNMP traps:

- 1 Click **Administration > SNMP > Traps > Remove**. The SNMP Traps Remove Page opens.

Figure 77 SNMP Traps Remove Page



The *SNMP Traps Remove* Page contains the following fields:

- **Remove** — Deletes the currently selected recipient. The possible field values are:
 - *Checked* — Removes the selected recipient from the list of recipients.
 - *Unchecked* — Maintains the list of recipients.
 - **Recipients IP** — Defines the IP address to which the traps are sent.
 - **Trap** — Displays the trap type. The possible field values are:
 - *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
 - *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
 - **Community String** — Defines the community string of the trap manager.
- 2 Select the SNMP trap to be deleted.
- 3 Click **Remove**. The SNMP trap is deleted, 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 are 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 Queuing Algorithm
- Viewing CoS to Queue
- Defining CoS to Queue
- Viewing DSCP to CoS
- Configuring DSCP to CoS
- Configuring Trust Settings
- Viewing Bandwidth Settings
- Defining Bandwidth Settings
- Defining Voice VLAN

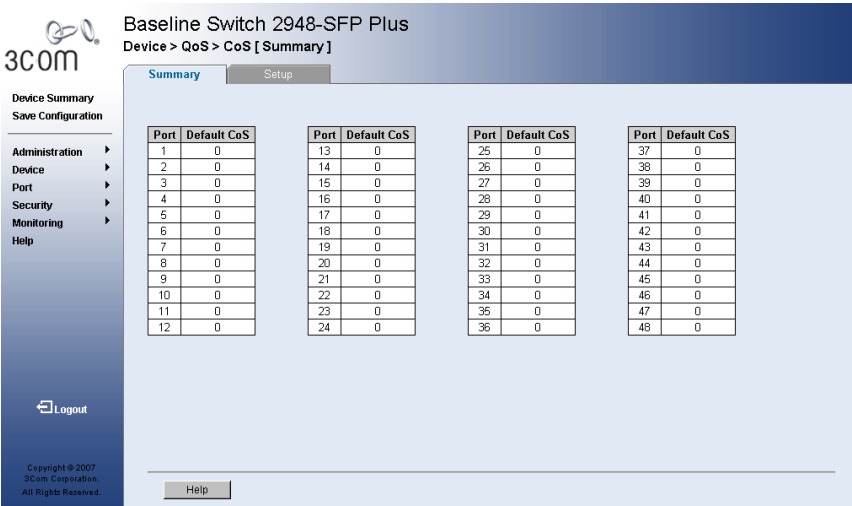
Viewing CoS Settings

The CoS Summary Page displays CoS default settings assigned to ports.

To view CoS Settings:

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

Figure78 CoS Summary Page



The CoS Summary Page contains the following fields:

- **Interface** — Displays the interface 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* contains information for enabling QoS globally.

Monitor users have no access to this page.

To configure CoS Settings:

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

Figure79 CoS Setup Page

Baseline Switch 2948-SFP Plus
Device > QoS > CoS [Setup]

Summary Setup

QoS Mode ☒ Enabled

Select Ports:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Select All Select None

☒ Set Default ☐ Restore Default

0

Help Apply Cancel

The *CoS Setup Page* contains the following fields:

- **QoS Mode** — Determines the QoS mode on the device:
 - *Disabled* — Disables QoS on the device.
 - *Enabled* — Enables QoS on the device.
 - **Select Port(s)** — Indicates the ports to be configured.
 - **Set Default** — Sets the default user priority. The possible field values are 0-7. The default CoS value is 0. With the default settings, 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 enabled on the device, and the device is updated.

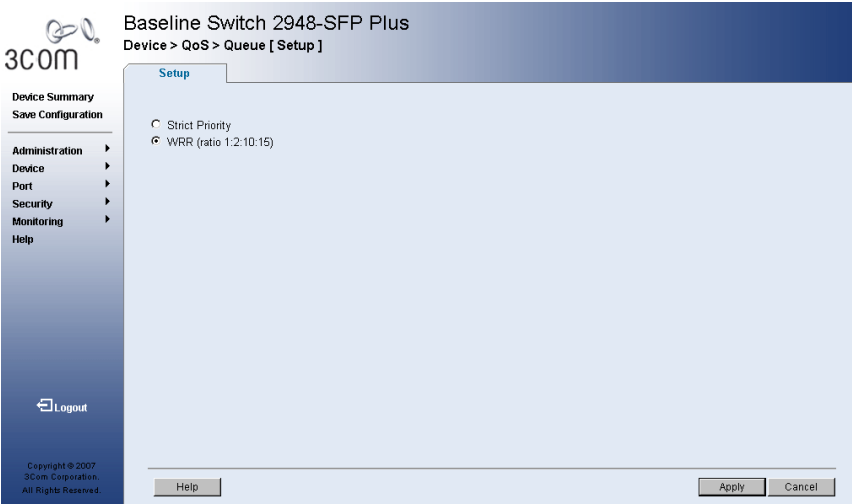
Defining Queuing Algorithm

The *Queue Setup Page* provides two scheduling methods: strict and weighted round robin (WRR).When QoS mode is disabled in the CoS Setup page, the scheduling method will be the default setting, WRR.
Monitor users have no access to this page

To configure Queue Settings:

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

Figure 80 Queue Setup Page



The *Queue Setup Page* contains the following fields:

- **Strict Priority** — Process the higher over the lower queues.
 - **WRR(ratio 1:2:15)** — Rotate service among the queues based on the weights assigned to each queues.
- 2 Define the fields.
 - 3 Click **Apply**. The queue is defined, and the device is updated.

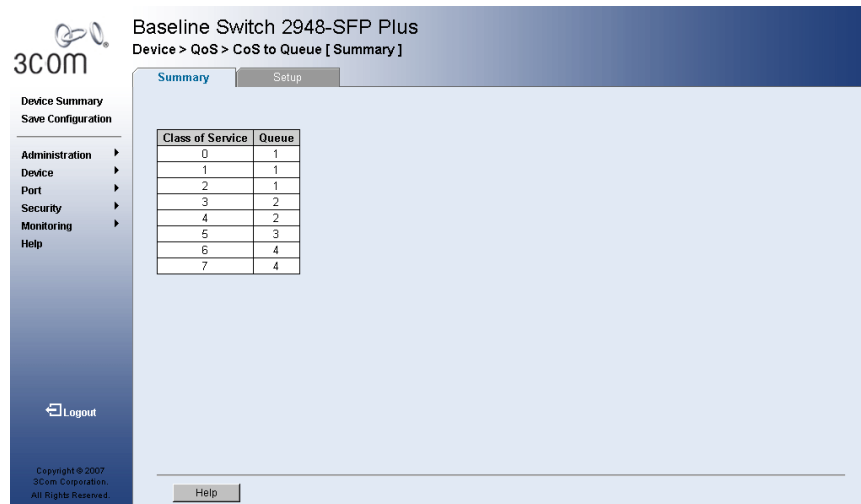
Viewing CoS to Queue

The *CoS to Queue Summary Page* contains a table that displays the CoS values mapped to traffic queues.

To view CoS Values to Queues:

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

Figure81 CoS to Queue Summary Page



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

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

Defining CoS to Queue

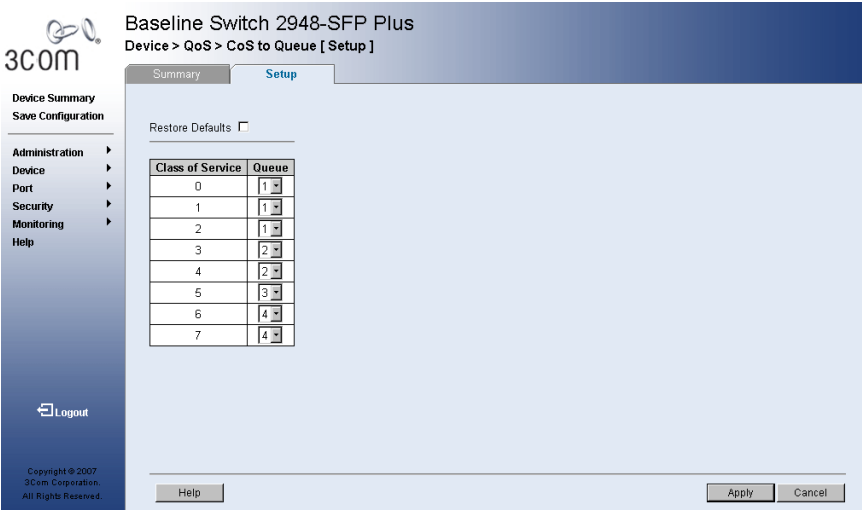
The *CoS to Queue Setup Page* contains fields for mapping CoS values to traffic queues. Four traffic priority queues are supported on the device, with 1 representing the lowest queue and 4 as the highest. The highest priority queue functions with strict priority. Queues 1-3 function with WRR priority with the following weights (1, 2 and 10) respectively.

The monitor user has 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 82 CoS to Queue Setup Page



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 zero 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

The *DSCP to CoS Summary Page* contains fields for mapping DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 4.

To view the DSCP Queue:

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

Figure 83 DSCP to CoS Summary Page

Baseline Switch 2948-SFP Plus
Device > QoS > DSCP to CoS [Summary]

Summary Setup

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

Help

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

- **DSCP** — Displays the incoming packet's DSCP value.
 - **Cos** — Specifies the value of CoS to which the DSCP priority is mapped for traffic forwarding. Eight (8) CoS are supported.
- 2 Define the queue number in the CoS field next to the required DSCP value.
 - 3 Click **Apply**. The DSCP values are mapped to CoS values, and the device is updated.

Configuring DSCP to CoS

The *DSCP to CoS Setup Page* contains fields for mapping DSCP settings to values of CoS. For example, a packet with a DSCP tag value of 3 can be assigned to CoS 1.

The monitor user has no access to this page.

To map DSCP to CoS :

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

Figure 84 DSCP to CoS Setup Page

Baseline Switch 2948-SFP Plus
Device > QoS > DSCP to CoS [Setup]

Summary Setup

Device Summary
Save Configuration

Administration >
Device >
Port >
Security >
Monitoring >
Help

Logout

Copyright © 2007
3Com Corporation
All Rights Reserved

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 value.
 - **CoS** — Specifies the value of CoS to which the DSCP priority is mapped for traffic forwarding. Eight (8) CoS are supported.
- 2 Define the queue number in the CoS field next to the required DSCP value.
 - 3 Click **Apply**. The DSCP values are mapped to CoS values, and the device is updated.

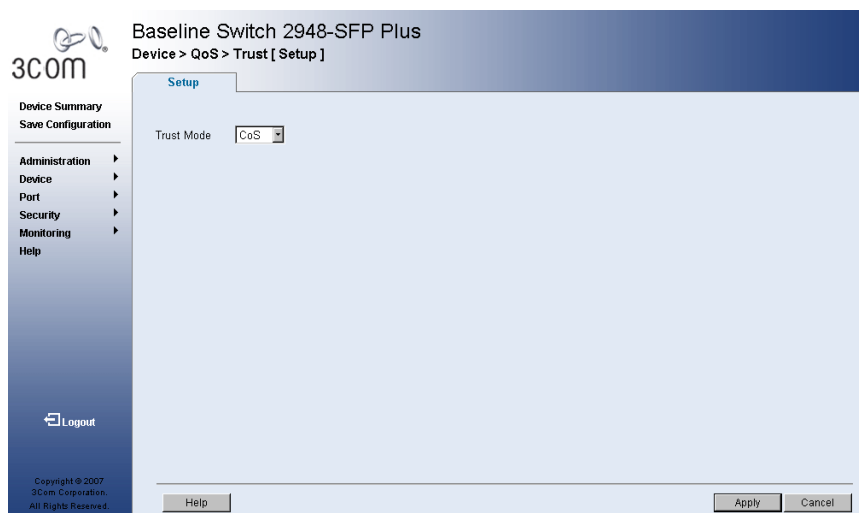
Configuring Trust Settings

The *Trust Setup Page* contains information for enabling trust on configured interfaces. The original device QoS default settings can be reassigned to the interface in the Trust Setup Page.

To enable Trust:

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

Figure 85 Trust Setup Page



The *Trust Setup Page* contains the following fields:

- **Trust Mode** — Defines which packet fields to use for classifying packets entering the device. When no rules are defined, the traffic containing the predefined packet CoS field is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to “best effort”. The possible Trust Mode field values are:
 - *CoS* — Classifies traffic based on the CoS tag value.
 - *DSCP* — Classifies traffic based on the DSCP tag value.
- 2 Define the fields.
 - 3 Click **Apply**. Trust mode is enabled on the device.

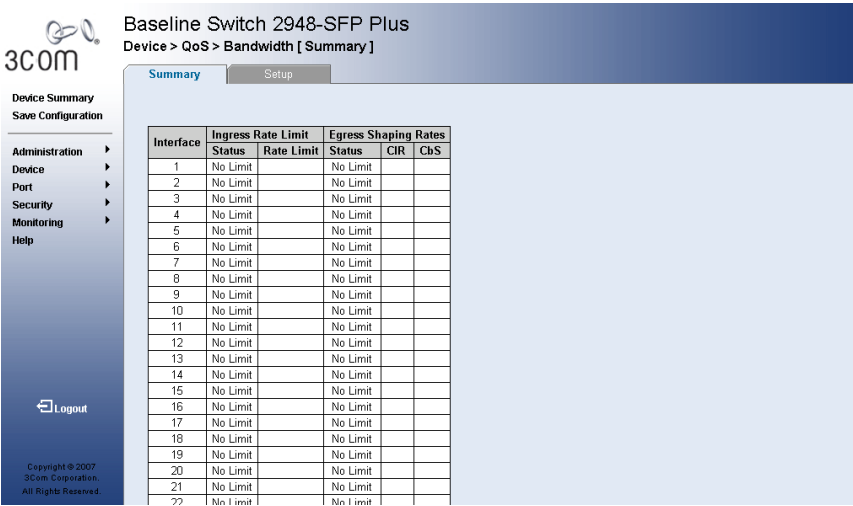
Viewing Bandwidth Settings

The *Bandwidth Summary Page* displays bandwidth settings for a specified interface.

To view Bandwidth Settings:

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

Figure 86 Bandwidth Summary Page



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 if rate limiting is defined on the interface. The possible field values are:
 - *Enable* — Enables ingress rate limiting on the interface.
 - *No Limit* — Ingress rate limiting is disabled on the interface.
- **Rate Limit** — Indicates the traffic limit for the port.

Egress Shaping Rates

- **Status** — Defines the shaping status. The possible field values are:
 - Enable — Egress rate limiting is enabled on the interface.
 - No Limit — Egress rate limiting is disabled on the interface.
- **CIR** — Indicates CIR as the interface shaping type.
- **CbS** — Indicates CbS as the interface shaping type.

Defining Bandwidth Settings

The *Bandwidth Setup Page* allows network managers to define the bandwidth settings for a specified interface. Interface shaping can be based on an interface and is determined by the lower specified value. The interface shaping type is selected in the Bandwidth Setup Page.

The monitor user has no access to this page.

To configure Bandwidth Settings:

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

Figure 87 Bandwidth Setup Page

3COM Baseline Switch 2948-SFP Plus
Device > QoS > Bandwidth [Setup]

Summary 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:

1	1	3	4	5	6	7	8	9	1	1	1	13	14	15	16	17	18	19	20	21	22	23	24	45	46
25	26	1	1	20	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	47	48

Select All Select None

Help Apply Cancel

Device Summary
Save Configuration

Administration
Device
Port
Security
Monitoring
Help

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

The *Bandwidth Setup Page* contains the following fields:

Ingress Rate Limit

- **Enable Ingress Rate Limit** — Enables setting an Ingress Rate Limit.
- **Ingress Rate Limit** — Indicates the traffic limit for the port. The possible field value is 128-500,032 kbits per second.

Egress Shaping Rate

- **Enable Egress Shaping Rate** — Enables Egress Shaping Rates.
- **Committed Information Rate (CIR)** — Defines CIR as the interface shaping type. The possible field value is 128-500,032 kbits per second.
- **Committed Burst Size (CbS)** — Defines CbS as the interface shaping type. The possible field value is 64-131,072 kbits per second.
- **Select ports** — Indicates the ports to be configured.
- **Select All** — Allows the user to assign the bandwidth settings to all ports.
- **Select None** — Removes the ports selected.

2 Select the ports to be configured.

3 Define the fields.

4 Click **Apply**. The bandwidth is defined, and the device is updated.

Defining Voice VLAN

Voice VLAN allows network administrators to enhance the 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 VLANs 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, ensuring that the quality of voice does not deteriorate if the 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 use the Voice VLAN and start sending tagged packets.

This section contains the following topics:

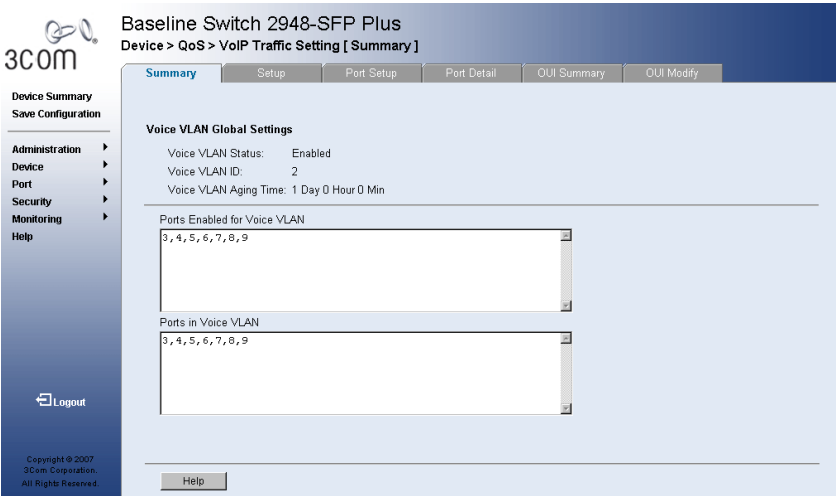
- Viewing Voice VLANs
- Defining Voice VLAN
- Defining Voice VLAN Port Settings
- Viewing Voice VLAN Port Definitions
- Viewing the OUI Summaries
- Modifying OUI Definitions

Viewing Voice VLAN The *Voice VLAN Summary Page* contains information about the Voice VLAN currently enabled on the device, including the ports enabled and included in the Voice VLAN.

To view Voice VLAN Settings:

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

Figure 88 Voice VLAN Summary Page



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

- **Voice VLAN State** — Indicates if Voice VLAN is enabled on the device. 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.
- **Voice VLAN Aging Time** — Indicates the amount of time after the last IP phone's OUI is aged out for a specific port. The port will age out after the bridge and voice aging time. The default time is one day. The field format is Day, Hour, Minute. The aging time starts after the MAC Address is aged out from the Dynamic MAC

Address table. The default time is 300 sec. For more information on defining MAC address age out time, see *Defining Aging Time*.

- **Ports Enabled for Voice VLAN** — Displays the ports on which Voice VLAN is enabled.
- **Ports in the Voice VLAN** — Displays the active ports which are included in the Voice VLAN currently.

Defining Voice VLANs

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

To configure Voice VLAN Settings:

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

Figure 89 Voice VLAN Setup Page

The screenshot displays the 'Voice VLAN Setup Page' for a 3Com Baseline Switch 2948-SFP Plus. The page is titled 'Device > QoS > VoIP Traffic Setting [Setup]'. It features a navigation menu on the left with options like 'Administration', 'Device', 'Port', 'Security', 'Monitoring', and 'Help'. The main content area is divided into tabs: 'Summary', 'Setup' (selected), 'Port Setup', 'Port Detail', 'OUI Summary', and 'OUI Modify'. Under the 'Setup' tab, the 'Voice VLAN Global Settings' section contains three fields: 'Voice VLAN Status' (a dropdown menu set to 'Enabled'), 'Voice VLAN ID' (a text box containing '2'), and 'Voice VLAN Aging Time' (a time selector set to '1 Day 0 Hour 0 Min (5 Min-30 Day)'). At the bottom of the page, there are 'Help', 'Apply', and 'Cancel' buttons.

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

- **Voice VLAN Status** — Indicates if Voice VLAN is enabled on the device. 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.
 - **Voice VLAN Aging Time** — Indicates the amount of time after the last IP phone's OUI is aged out for a specific port. The port will age out after the bridge and voice aging time. The default time is one day. The field format is Day, Hour, Minute. The aging time starts after the MAC Address is aged out from the Dynamic MAC Address table. The default time is 300 sec. For more information on defining MAC address age out time, see Defining Aging Time.
- 2 Select Enable in the Voice VLAN State field.
 - 3 Define the Voice VLAN and Voice VLAN Aging Time fields.
 - 4 Click **Apply**. The Voice VLAN is defined, and the device is updated.

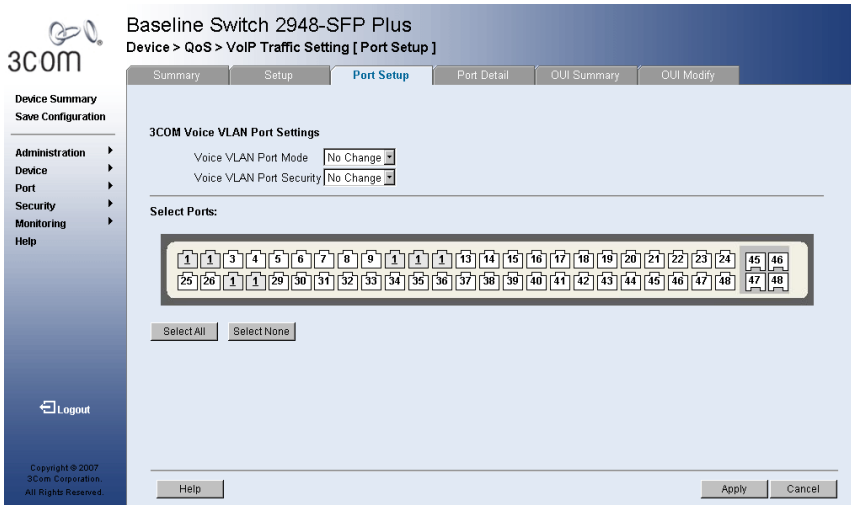
Defining Voice VLAN Port Settings

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

To configure Voice VLAN port settings:

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

Figure 90 Voice VLAN Port Setup Page



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

- **Voice VLAN Port Mode** — Defines the Voice VLAN mode. The possible field values are:
 - *No Changes* — Maintains the current Voice VLAN port settings. This is the default value.
 - *None* — Indicates that the selected port will not be added to a Voice VLAN.
 - *Manual* — Adding a selected port to a Voice VLAN.
 - *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 IP phone's MAC address (with an OUI prefix) is aged out and exceeds the defined Voice VLAN Aging Time in the setup page.
- **Voice VLAN 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.
 - *No Changes* — Maintains the current Voice VLAN port security settings.
 - *Enabled* — Enables port security on the Voice VLAN.
 - *Disabled* — Disables port security on the Voice VLAN. This is the default value.
- **Select Port** — Enables selecting specific ports to which the Voice VLAN settings are applied.
 - *Selected (Blue)* — Indicates that the port is selected, and Voice VLAN settings are applied to the port.
 - *Unselected* — Indicates that the port is not selected, and the Voice VLAN settings are not applied to the port. This is the default value.
 - *Select All* — Allows the user to assign the Voice VLAN settings to all ports.
 - *Select None* — Removes the ports selected.

- 2 Click a port in the Zoom View. The port is highlighted in 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.

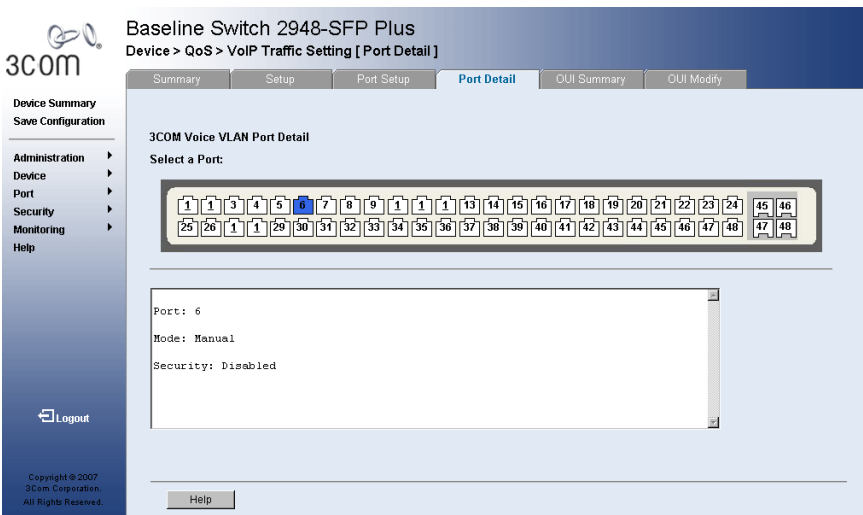
Viewing Voice VLAN Port Definitions

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 91 Voice VLAN Port Details Page



- 2 Click a port in the Zoom View. The port is highlighted in blue, and the Voice VLAN port settings are displayed in the text box.

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

- **Select a Port** — Select a port for displaying the current Voice VLAN port settings. VLAN port definitions are applied.
- **Port** — Displays the Voice VLAN Port Details for a selected port.
- **Mode** — Defines the Voice VLAN mode. The possible field values are:
 - *None* — Indicates that the selected port will not be added to a Voice VLAN.
 - *Manual* — Adding a selected port to a Voice VLAN.
 - *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 IP phone's MAC address (with an OUI prefix) is aged out and exceeds the defined Voice VLAN Aging Time in the setup page.
- **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.

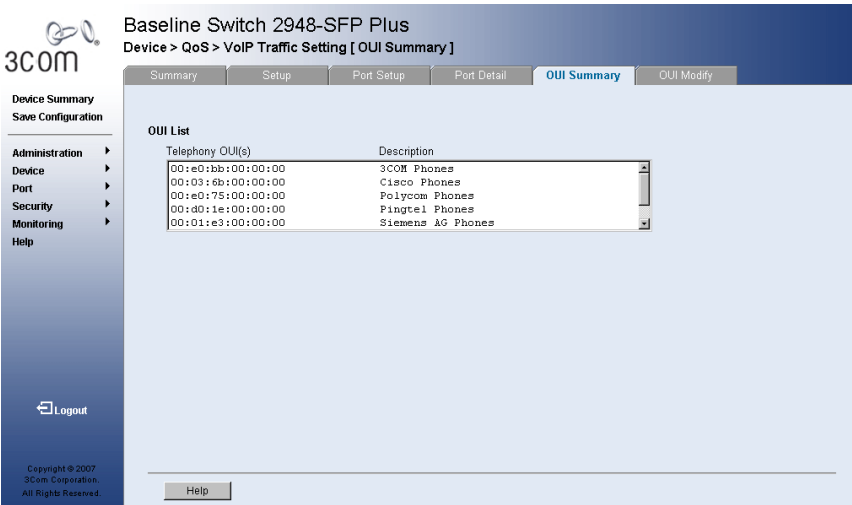
Viewing the OUI Summaries

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. 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 VLAN Settings:

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

Figure 92 Voice VLAN OUI Summary Page



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/Veritel IP Phones.
 - 00:D0:1E — Assigned to Pingtel IP Phones.
 - 00:01:E3 — Assigned to Siemens IP Phones.
 - 00:60:B9 — Assigned to NEC/Philips IP Phones.
 - 00:0F:E2 — Assigned to H3C IP Phones.
- **Description** — Provides an 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 on the MAC address and is manufacture specific. 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 specific manufacture'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 modify OUI Settings:

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

Figure 93 Voice VLAN OUI Modify Page

Baseline Switch 2948-SFP Plus
Device > QoS > VoIP Traffic Setting [OUI Modify]

Summary Setup Port Setup Port Detail OUI Summary **OUI Modify**

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

Telephony OUI (3 MSB MAC Address only)
Description

Add Remove

Telephony OUI(s)	Description
00:e0:bb:00:00:00	3COM Phones
00:03:6b:00:00:00	Cisco Phones
00:e0:75:00:00:00	Polycom Phones
00:d0:1e:00:00:00	Pingtel Phones
00:01:e3:00:00:00	Siemens AG Phones
00:60:b9:00:00:00	Phillips and NEC AG Phones
00:0f:e2:00:00:00	H3c Aolynk Phones
ff:ff:ff:00:00:00	

Help Cancel

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

- **Telephony OUI** — Defines new OUIs enabled on the Voice VLAN.
 - **Description** — Provides a user-defined OUI description (up to 32 characters).
- 2 Defines or selects the relative field.
 - 3 Click **"Add"** or **"Remove"**, and the device is updated.

14

MANAGING SYSTEM FILES

This section contains information about managing the configuration files and installing and backing up the switch firmware. This section includes the following topics:

- Configuration File Structure
- Backing Up System Files
- Restoring Files
- Upgrade the Firmware Image
- Activating Image Files

Configuration File Structure

The configuration file structure consists of the following:

- **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 from via TFTP or HTTP.
- **Running Configuration File** — Contains all configuration file commands, and all commands entered during the current session. When the device is powered down or rebooted, the commands in the Running Configuration file are lost. During startup, all commands in the Startup file are copied to the Running Configuration File and applied to the device. To update the Startup file, click the Save Configuration button before powering down the device. This copies the Running Configuration file to 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 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 Config file.

Backing Up System Files

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

The monitor users have no access to this page.

- 1 To keep your currently running configuration, click the **Save Configuration** item on the left side of the page.
- 2 Click **Administration > Backup & Restore > Backup**. The *Backup Page* opens.

Figure 94 Backup Page

The *Backup Page* contains the following fields:

- **Upload via TFTP** — Enables initiating an upload to the TFTP server.
 - **Upload via HTTP** — Enables initiating an upload to the HTTP client or HTTPS client.
 - **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the configuration files are uploaded.
 - **Destination File Name** — Specifies the destination file to which the configuration file is uploaded.
- 3 Define the relevant fields.
 - 4 Click **Apply**. The backup file is defined, and the device is updated.

Restoring Files

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

The monitor users have no access to this page.

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

Figure 95 Restore Page

Baseline Switch 2948-SFP Plus
Administration > Backup & Restore [Restore]

Backup Restore

☒ Download via TFTP
☐ Download via HTTP

Configuration Upload

TFTP Server IP Address

Source File Name

Help OK Cancel

The *Restore Page* contains the following fields:

- Download via TFTP — Enables a download from the TFTP server.
- Download via HTTP — Enables a download from the HTTP client or HTTPS client.

Configuration Download

- TFTP Server IP Address — Specifies the TFTP Server IP Address from which the configuration files are 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.

Upgrade the Firmware Image



The *Restore Image Page* permits network managers to upgrade the switch firmware.

- Note: The bootcode can only be upgraded using the Command Line Interface (CLI). See “*Upgrading Software using the CLI*”.
- The monitor user has no access to this page.

To download the software image:

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

Figure 96 Restore Image Page

The *Restore Image Page* contains the following fields:

- **Download via TFTP** — Enables initiating a download via the TFTP server.
 - **Download via HTTP** — Enables initiating a download via the HTTP client or HTTPS client.
 - **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which the image files are 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.

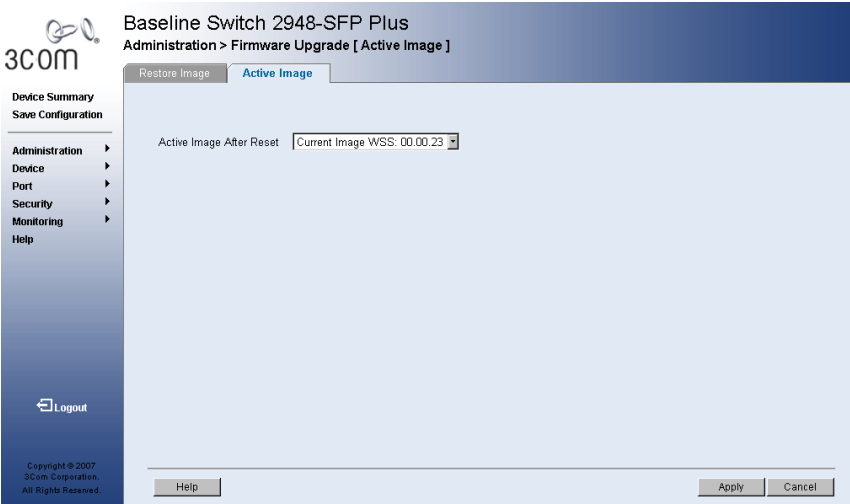
Activating Image Files

The *Active Image Page* allows network managers to select and reset the Image files.

To upload System files:

- 1 Click **Administration > Firmware Upgrade > Active Image**. The *Active Image Page* opens.

Figure 97 Active Image Page



The *Active Image Page* contains the following fields:

- **Active Image After Reset** — The Image file which is active on the unit after the device is reset. The possible field values are:
 - **Current Image** — Activates the current image after the device is reset.
 - **Backup Image** — Activates backup image after the device is reset.
- 2 Select the active image to be activated after reset.
 - 3 Click **Apply**. The active image file is defined, and the device is updated.

15

VIEWING STATISTICS

This section contains information about 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 RMON statistics:

- 1 Click **Ports > Statistics > Summary**. The *Port Statistics Summary Page* opens.

Figure 98 Port Statistics Summary Page

3COM Baseline Switch 2948-SFP Plus
Port > Statistics [Summary]

Summary

Select a Port:

Refresh Rate: No Refresh Clear All Counters

Received Bytes (Octets)	9991244
Received Packets	115161
Broadcast Packets Received	79693
Multicast Packets Received	399
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	125413
Frames of 65 to 127 Bytes	40098
Frames of 128 to 255 Bytes	5667
Frames of 256 to 511 Bytes	3330
Frames of 512 to 1023 Bytes	2903
Frames of 1024 to 1518 Bytes	7192

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

- **Select a Port** — Defines the specific port for which RMON statistics are displayed.

- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the port statistics are not refreshed.
 - *15 Sec* — Indicates that the port statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the port statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the port statistics are refreshed every 60 seconds.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
 - **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
 - **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
 - **Frames of 64 Bytes** — Number of 64-byte frames received on the interface since the device was last refreshed.
 - **Frames of 65 to 127 Bytes** — Number of 65 to 127 byte frames received on the interface since the device was last refreshed.
 - **Frames of 128 to 255 Bytes** — Number of 128 to 255 byte frames received on the interface since the device was last refreshed.
 - **Frames of 256 to 511 Bytes** — Number of 256 to 511 byte frames received on the interface since the device was last refreshed.
 - **Frames of 512 to 1023 Bytes** — Number of 512 to 1023 byte frames received on the interface since the device was last refreshed.
 - **Frames of 1024 to 1518 Bytes** — Number of 1024 to 1518 byte frames received on the interface since the device was last refreshed.
- 2 Select a port. The port statistics are displayed.
 - 3 Click **Clear All Counters**. The port statistics counters are cleared and the new statistics are displayed.

16

MANAGING DEVICE DIAGNOSTICS

This section contains information for viewing and configuring port and cable diagnostics, and includes the following topics:

- Configuring Port Mirroring
- Viewing Cable Diagnostics

Configuring Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators can configure port mirroring by selecting a specific port from which to copy all packets, and other ports to which the packets copied.

The monitor user has limited access to this page.

This section contains the following topics:

- Defining Port Mirroring
- Removing Port Mirroring

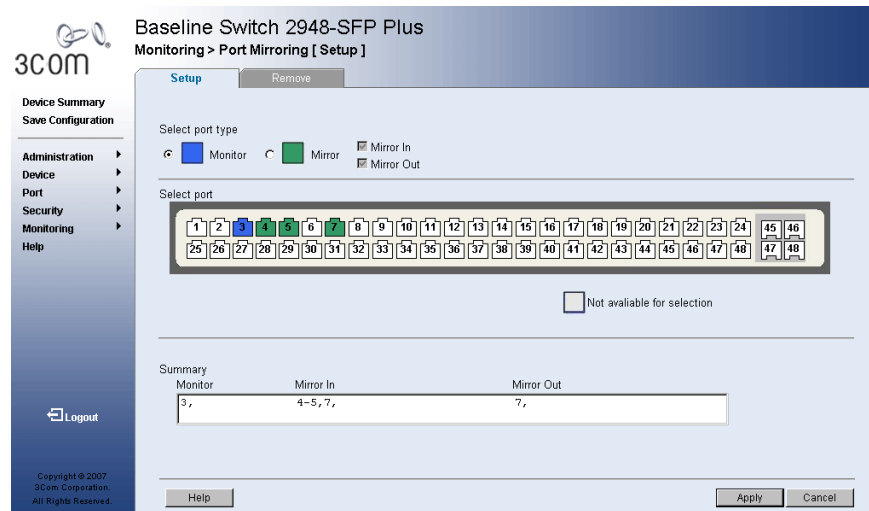
Defining Port Mirroring

The *Port Mirroring Setup Page* contains parameters for configuring port mirroring.

To enable port mirroring:

- 1 Click **Monitoring > Port Mirroring > Setup**. The *Port Mirroring Setup Page* opens.

Figure 99 Port Mirroring Setup Page



Baseline Switch 2948-SFP Plus
Monitoring > Port Mirroring [Setup]

Setup Remove

Select port type
☒ Monitor ☐ Mirror ☐ Mirror In ☐ Mirror Out

Select port

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

☐ Not available for selection

Summary

Monitor	Mirror In	Mirror Out
3,	4-5, 7,	7,

Help Apply Cancel

Copyright © 2007 3Com Corporation. All Rights Reserved.

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 or the destination port.
 - *Mirror* — Defines the port as the mirrored port to be monitored and indicates the traffic direction to be monitored. If selected, the possible values are:
 - *Mirror In* — Enables port mirroring on the port RX.
 - *Mirror Out* — Enables port mirroring on the port TX.

- **Select port** — Selects the port for mirroring or monitoring. A port unavailable for mirroring is colored grey.
 - **Summary** — Displays the current monitor and mirror ports. The fields displayed are:
 - *Monitor* — Displays the monitor port.
 - *Mirror In* — Displays ports that are monitored on the RX.
 - *Mirror Out* — Displays ports that are monitored on the TX.
- 2 Select a port type.
 - 3 If the Mirrored port type is selected, select Mirror In or Mirror Out.
 - 4 Select the ports to be monitored.
 - 5 Click **Apply**. Port mirroring is enabled, and the device is updated.

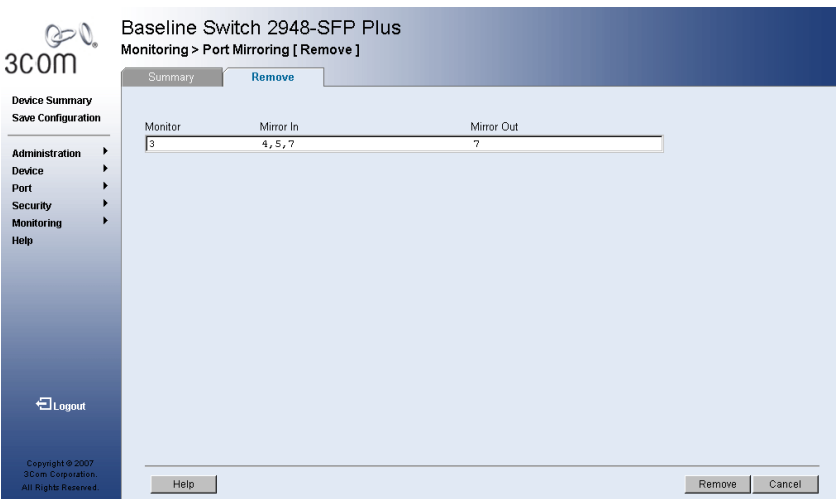
Removing Port Mirroring

The *Port Mirroring Remove Page* permits the network manager to terminate port mirroring or monitoring.

The monitor users have no access to this page.

- 1 Click **Monitoring > Port Mirroring > Remove**. The *Port Mirroring Remove Page* opens.

Figure 100 Port Mirroring Remove Page



The *Port Mirroring Remove Page* contains the following fields:

- **Monitor** — Displays the monitor port.
 - **Mirror In** — Displays ports that are monitored on the RX.
 - **Mirror Out** — Displays ports that are monitored on the TX.
- 2 Select the ports to be removed.
 - 3 Click **Remove**. Port mirroring is removed, and the device is updated.

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, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port.

The monitor users have limited access to this page.

To view cables diagnostics:

Click **Monitoring > Cable Diagnostics > Summary**. The *Cable Diagnostics Summary Page* opens.

Figure 101 Cable Diagnostics Summary Page

Baseline Switch 2948-SFP Plus
Monitoring > Cable Diagnostics [Summary]

Summary | Diagnostics

Port	Test Result	Cable Fault Distance	Last Update
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

Device Summary
Save Configuration

Administration >
Device >
Port >
Security >
Monitoring >
Help

Logout

Copyright © 2007
3Com Corporation.
All Rights Reserved.

The *Cable Diagnostics Summary Page* contains the following fields:

- **Ports** — Specifies the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
 - *Open* — Indicates a cable is not connected, or the cable is connected on only one side, or the cable is shorter than 1 meter.
 - *Short* — Indicates that a short has occurred in the cable.
 - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred, in meters.
- **Last Update** — Indicates the last time the port was tested.

Configuring Cable Diagnostics

The *Diagnostics Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error, which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port.

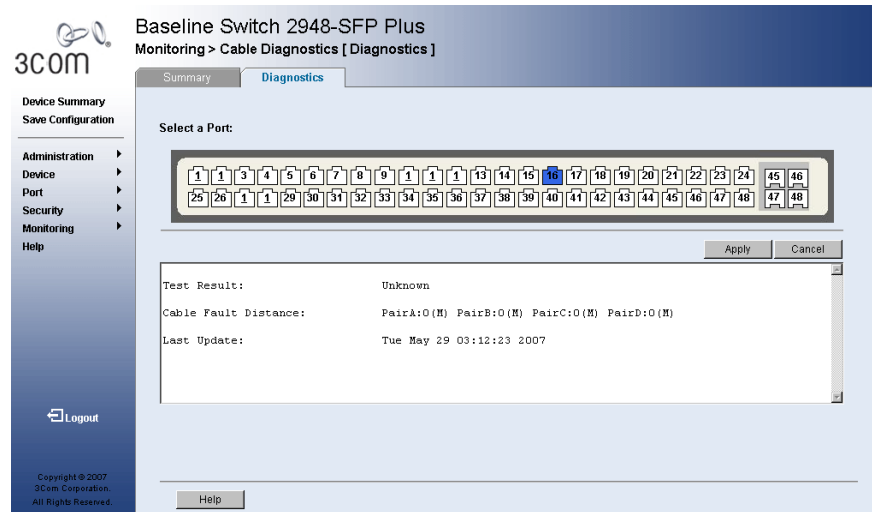
When performing cable tests consider the following:

- During the tests, ports are in the down state.
- The minimum cable length resolution is one meter, so if the cable is shorter than 1 meter the test will display “no cable”.
- An open cable or a 2-pair copper cable will display a cable fault distance of 0.
- The maximum cable length is 120 meters.

To test cables:

- 1 Click **Monitoring > Cable Diagnostics > Diagnostics**. The *Diagnostics Page* opens.

Figure 102 Diagnostics Page



The *Diagnostics Page* contains the following fields:

- **Select a Port** — Specifies the port to be tested.
- **Test Result** — Displays the cable test results. Possible values:
 - *Open* — Indicates that a cable is not connected to the cable but is either connected on only one side or the cable is 1 meter.
 - *Short* — Indicates that a short has occurred in the
 - *OK* — Indicates that the cable passed the test.

- **Cable Fault Distance** — Indicates the distance from where the cable error occurred.

A Cable Fault Distance of 0 can result from a short (<1m) cable, cable or a 2-pair copper cable.

- **Last Update** — Indicates the last time the port was tested.

- 2 Select a port to be tested.

- 3 Click **Apply**. The ports are tested, and the page is updated.

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 RADIUS 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 Standard	The 3Com® Baseline Switch 2948-SFP Plus has been designed to the following standards:	
	Function	8802-3, IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab (Gigabit Ethernet), IEEE 802.1D (Bridging)
	Safety	UL 60950-1, EN 60950-1, CSA 22.2 No. 60950-1, IEC 60950-1
	EMC Emissions	EN55022 Class A, CISPR 22 Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, EN61000-3-2, EN61000-3-3.
	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 cm (10.43 in.)
	Height	44 mm (1.73 in.) or 1U.
	Weight	2.0 kg (4.4 lb)
	Mounting	Free-standing, or 19 in. rack-mounted using the supplied mounting kit

Electrical	Line Frequency	50/60 Hz
	Input Voltage	100–240 Vac (auto range)
	Current Rating	
	Switch 2948-SFP Plus	1.5 Amp (Max)
	Maximum Power Consumption	
	Switch 2948-SFP Plus	70 Watts
	Max Heat Dissipation	
	Switch 2948-SFP Plus	238.9 BTU/hr

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

Table 11 Features of the Baseline Switch 2948-SFP Plus

Feature	Description
Auto-Negotiation	<p>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.</p> <p>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:</p> <ul style="list-style-type: none">■ 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

Table 11 Features of the Baseline Switch 2948-SFP Plus

Feature	Description
Automatic MAC Addresses Aging	MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.
Back Pressure	On half duplex links, the receiver may employ back pressure (i.e. occupy the link so it is unavailable for additional traffic), to temporarily prevent the sender from transmitting additional traffic. This is used to prevent buffer overflows.
Address Resolution Protocol (ARP)	ARP converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.
Class Of Service (CoS)	Provide traffic belonging to a group preferential service (in terms of allocation of system resources), possibly at the expense of other traffic.
Command Line Interface	The Command Line Interface (CLI) is an interface using a serial connection that allows basic features to be configured, including IP address management and firmware upgrading. The CLI is not intended as the main interface for the switch.
Configuration File Management	The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.
DHCP Clients	Dynamic Host Client Protocol. DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process.
Fast Link	STP can take up to 30-60 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies where forwarding loops do not occur.
Full 802.1Q VLAN	IEEE 802.1Q defines an architecture for virtual bridged LANs, the Tagging Compliance 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.

Table 11 Features of the Baseline Switch 2948-SFP Plus

Feature	Description
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.
Link Aggregated Groups	<p>Link Aggregated Group (LAG). The system provides up-to eight Aggregated Links to be defined, each with up to eight member ports, to form a single LAG. LAGs provide:</p> <ul style="list-style-type: none">■ Fault tolerance protection from physical link disruption■ Higher bandwidth connections■ Improved bandwidth granularity■ High bandwidth server connectivity■ LAG is composed of ports with the same speed, set to full-duplex operation.
MAC Address Capacity Support	The device supports up to 8K MAC addresses. The device reserves specific MAC addresses for system use.
MAC Multicast Support	Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 Multicast service is where a single frame is addressed to a specific Multicast address, from where copies of the frame are transmitted to the relevant ports.
MDI/MDIX Support	The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).
Password Management	Password management provides increased network security and improved password control. Passwords for HTTP, HTTPS, and SNMP access are assigned security features. For more information on Password Management, see “Default Users and Passwords”.
Port-based	Port-based authentication enables authenticating system users on a Authentication 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).

Table 11 Features of the Baseline Switch 2948-SFP Plus

Feature	Description
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.
RADIUS Clients	RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password, and accounting information.
Rapid Spanning Tree	Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.
Remote Monitoring	Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.
Self-Learning MAC Addresses	The device enables automatic MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table.
SNMP Alarms and Trap Logs	The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.
SNMP Versions 1 and 2	Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the system.
Spanning Tree Protocol	802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.
SSL	Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.
Static MAC Entries	MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user defined entries are not subject to aging, and are preserved across resets and reboots.

Table 11 Features of the Baseline Switch 2948-SFP Plus

Feature	Description
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

Console Cable

A Console cable is an 8-conductor RJ45-to-DB9 cable. One end of the cable has an RJ-45 plug for connecting to the switch's Console port, and the other end has a DB-9 socket connector for connecting to the serial port on the terminal, as shown in Figure 102.

Figure 102 Console cable

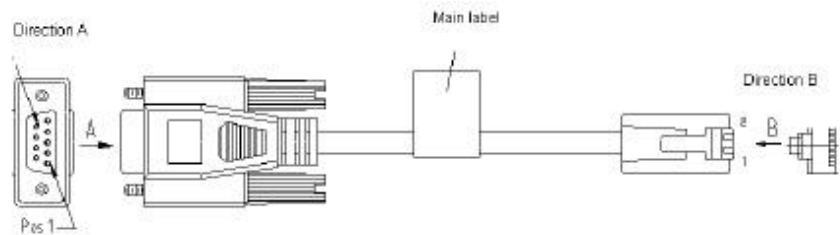
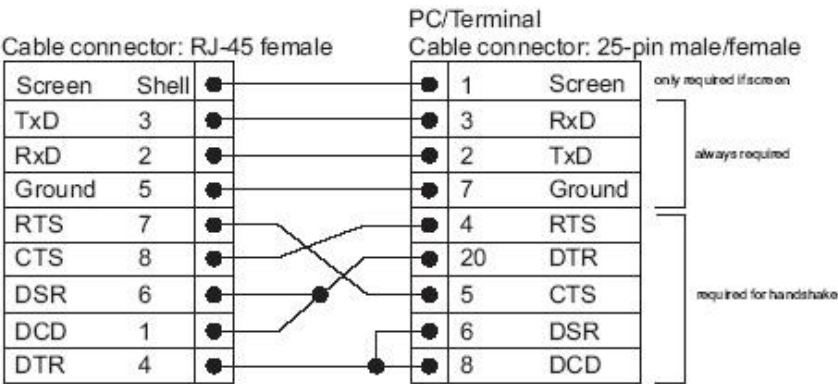


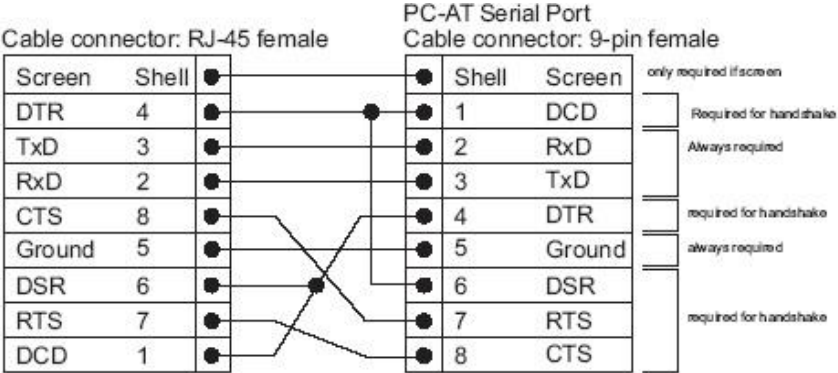
Table 12 Console cable pinouts

RJ-45	Signal	Direction	DB9 (modem)	DB9 (console)
1	RTS	—	7	8
2	DTR	—	4	4
3	TXD	—	3	2
4	CD	—	1	5
5	GND	—	5	5
6	RXD	—	2	3
7	DSR	—	6	4
8	CTS	—	8	7

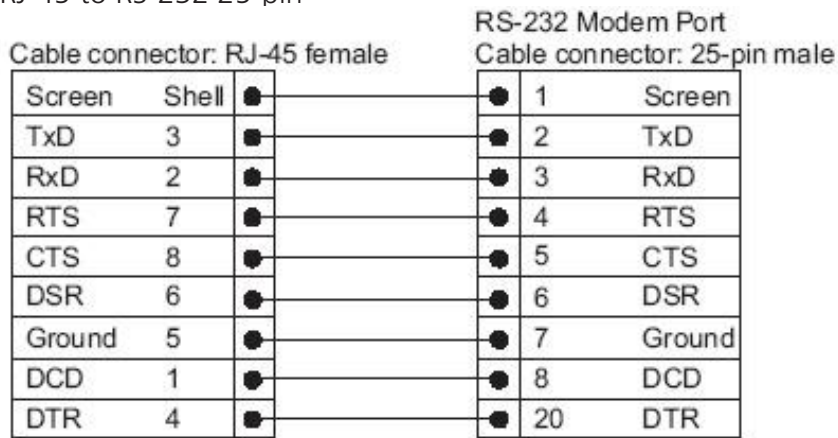
Null Modem Cable RJ-45 to RS-232 25-pin



PC-AT Serial Cable RJ-45 to 9-pin



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



Ethernet Port RJ-45
Pin Assignments

10/100 and 1000BASE-T RJ-45 connections.

Table 10 Pin assignments

Pin Number	10/100	1000
<i>Ports configured as MDI</i>		
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
<i>Ports configured as MDIX</i>		
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 switch and how to resolve these issues. This section includes the following topics:

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

Problem Management

Problem management includes isolating problems, quantifying the problems, and then applying the solution. When a problem is detected, the exact nature of the problem must be determined. This includes how the problem is detected, and 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:

- Switch does not run; power LED is off.
- Cannot connect to management using Console connection
- Cannot connect to switch management using HTTP, SNMP, etc.
- Self-test exceeds 15 seconds
- No connection is established and the port LED is on
- Device is in a reboot loop
- No connection and the port LED is off
- Lost Password.

Table 12 Troubleshooting Solutions

Problems	Possible Cause	Solution
Switch does not run; power LED is off.	Power is disconnected.	Verify that the power cord is properly connected to the switch, and to the mains supply.
Cannot connect to management using Console 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, the default gateway is configured. Check that your cable is properly connected with a valid link light, and that the port has not been disabled. Ensure that your management station is plugged into the appropriate VLAN to manage the device. If you cannot connect using the web, the maximum number of connections may already be open. Try again at a later time.
No response from the terminal emulation software	Faulty serial cable Incorrect serial cable Software Settings	Replace the serial cable. Replace the serial cable for a pin-to-pin straight/flat cable. Reconfigure the emulation software connection settings.
Response from the terminal emulation software is not readable	Faulty serial cable Software Settings	Replace the serial cable. Reconfigure the emulation software connection settings.
Self-test exceeds 15 seconds	The device may not be correctly installed.	Remove and reinstall the device. If that does not help, consult your technical support representative.
No connection is LED established and the port 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	Replace the module.
	Faulty module	Replace the module.
	Incorrect initial configuration	Erase the connection and reconfigure the port.

Table 12 Troubleshooting Solutions

Problems	Possible Cause	Solution
Device is in a reboot loop	Software fault	Download and install a working or previous software version from the console.
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 10 Mbps connections use a Cat 5 cable. Check the port LED or zoom screen in the NMS application, and change setting if necessary.
Lost Password		Contact 3Com

E

3Com CLI REFERENCE GUIDE

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

Getting Started with the Command Line Interface

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

Console Port To start using the CLI via a console port:

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

Console Port Logging on to the CLI: The Login process requires a User Name and Password. The default user name for first time configuration is **admin**. No password is required. User names and passwords are case sensitive.

To logon to the CLI Interface:

- 1 Press **Enter** without typing in a username. The **Login** prompt displays:

Login:

- 2 Enter your **User Name** at The **Login** prompt.

3 Press **Enter**. The **Password** prompt display

```
Password:
```

The Login information is verified, and displays the following CLI menu:

```
Select menu option:
```

If the password is invalid, the following message appears and Login process restarts.

```
Incorrect Password
```

Automatic Logout The user session is automatically terminated after 30 minutes in which no device configuration activity has occurred. The following message is displayed:

```
Session closed by automatic logout.
```

Concurrent CLI Sessions The command line interface supports one CLI session.

CLI Commands

This Command section contains the following commands:

- ?
- initialize
- ipSetup
- logout
- ping
- password
- reboot
- summary
- upgrade

? The **?** command displays a list of CLI commands on the device.

Syntax

?

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

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

Select menu option?	
?	Displays Help information.
initialize	Reset the device to factory default, except IP.
ipSetup	Configures IP address.
logout	Logout from this session.
ping	Ping a remote station.
password	Change password.
reboot	Power cycles the device.
summary	Summarizes IP setup and software versions.
upgrade	Software upgrade over TFTP.

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

Syntax **ping**

Parameters

- IP Address — IP address to ping.

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

The following displays current IP configuration and software versions running on the device:

```
Select menu option: ping
Ping server 10.6.150.75
64 bytes from 10.6.150.75: icmp_seq=0 time=0ms
64 bytes from 10.6.150.75: icmp_seq=1 time=10ms
64 bytes from 10.6.150.75: icmp_seq=2 time=0ms
64 bytes from 10.6.150.75: icmp_seq=3 time=0ms
Sent 4 packets, received 4 OK, lost 0 packets,
```

Summary

The **Summary** command displays the current IP configuration and software versions running on the device. It is intended for devices that support separate runtime and bootcode Images.

Syntax

summary

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

The following displays current IP configuration and software versions running on the device:

```
Select menu option: Summary
IP Method:      Manual
IP address:     1.2.3.4
Subnet mask:    255.255.255.0
Default gateway: 4.3.2.1
Runtime version: example1.ext
Bootcode version: example2.ext
```

ipSetup The **ipSetup** command allows the user to define an IP address on the device either manually or via a DHCP server.

Syntax
ipSetup

Parameters

- **auto** — Specifies the IP address is acquired automatically from the Dynamic Host Configuration Protocol (DHCP) server.
- **manual** — Specifies the IP address.
- **ip-address mask**— Specifies that the IP address and default gateway are configured manually by the user (Range: 0.0.0.0 - 223.255.255.255).

Default Configuration

No default IP address is defined for interfaces.

User Guidelines

IP Addresses configured beyond the range of 224.0.0.0 are defined as multicast, experimental or broadcast addresses.

If a default gateway is configured manually, the IP-address and mask are required to be the same as the gateway-address and mask.

Example

The following example displays an IP address configured manually:

IpSetup Enter configuration method(auto,manual):	manual
Enter Ip address [169.254.3.64]:	192.168.1.1
Enter subnet mask [255.255.255.0]:	255.255.255.0
Enter gateway IP address [192.168.1.254]	192.168.1.254

The following example displays an IP address obtained via a DHCP server:

ipSetup Enter configuration method (auto,manual):	auto
---	------

Upgrade The **Upgrade** command starts a system download and thereby allowing a system upgrade.

Syntax **upgrade**

Parameters

- TFTP Server IP Address — Defines the TFTP server's IP address.
- Source File Name — Specifies the source file name.

Default Configuration

This command has no default configuration.

User Guidelines

During the upgrade process, a series of dots appear representing the upgrade process in the CLI interface. When the upgrade process is completed, the command prompt reappears.

The Dual Software Image feature is supported. Therefore the next boot after upgrade command will always use the newly downloaded image.

Intialize The **Initialize** command resets the device configuration to factory defaults, including the IP configuration.

Syntax
initialize

Default Configuration

This command has no default configuration.

User Guidelines

The system prompts for confirmation of the request. If no response is entered within 15 seconds, timeout occurs and the command is not executed.

Example

```
Select menu option: initialize

WARNING: This command initializes the system to factory
defaults (excluding IP details) and causes a reset.

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

Select menu option
```

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

Syntax
reboot

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

```
Select menu option: reboot
Are you sure you want to reboot the system (yes,no)[no]: no
Select menu option:
```

Layout The **Logout** command terminates the CLI session.

Syntax
logout

Default Configuration

This command has no default configuration.

User Guidelines

There are no user guidelines for this command.

Example

```
Select menu option: logout
exiting session...
Login:
```

Password The Password command changes the user's password.

Syntax
password

Default Configuration

This command has no default configuration.

User Guidelines

The user needs to login to the session in order to change the password.

Example

```
Select menu option: password
Change password for user: username
Old password:
Enter new password:
Retype password:
The command line interface password has been successfully
changed.
Select menu option:
```

F

GLOSSARY

- Access Control Entries (ACE)** ACEs are made of the filters that determine traffic classifications.
- 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. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.
- 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.
- Committed Information Rate (CIR)** CIR is a committed rate in bits-per-second at which the carrier agrees to accept packets from the client over a virtual circuit. The packets that are sent in excess of the CIR rate, become eligible to be discarded and not delivered if the frame relay network becomes congested, and it would then be necessary to resend these discarded packets.
- Committed Burst Size (Cbs)** CbS is the maximum number of bits that can be transferred over a frame relay link during some time interval.
- 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. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or 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 Multicast Registration Protocol (GMRP) GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

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 802.1s An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

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 802.3ac	Defines frame extensions for VLAN tagging.
IEEE 802.3x	Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.
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 or VLAN.
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.
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.
Private VLANs	Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Protected Extensible Authentication Protocol (PEAP)	<p>A protocol proposed by Microsoft, Cisco and RSA Security for securely transporting authentication data, including passwords, over 802.11 wireless networks. Like the competing standard Tunneled Transport Layer Security (TTLS), PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs.</p> <p>Protocol-Independent Multicasting (PIM)</p> <p>This multicast routing protocol floods multicast traffic downstream, and calculates the shortest-path back to the multicast source network via reverse path forwarding. PIM uses the router's IP routing table rather than maintaining a separate multicast routing table as with DVMRP. PIM - Sparse Mode is designed for networks where the probability of a multicast client is low, such as on a Wide Area Network. PIM – Dense Mode is designed for networks where the probability of a multicast client is high and frequent flooding of multicast traffic can be justified.</p>
Remote Authentication Dial-in User Service (RADIUS)	<p>RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.</p>
Remote Monitoring (RMON)	<p>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.</p>
Rapid Spanning Tree Protocol (RSTP)	<p>RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.</p>
Secure Shell (SSH)	<p>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.</p>
Routing Information Protocol (RIP)	<p>The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.</p>
Simple Network Management Protocol (SNMP)	<p>The application protocol in the Internet suite of protocols which offers network management services.</p>

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.
Terminal Access Controller Access Control System Plus (TACACS+)	TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on 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.

G

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

To take advantage of warranty and other service benefits, you must first register your product at: <http://eSupport.3com.com/>

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

3Com offers the following support tool:

- 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 your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced 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. For more information on 3Com Extended Warranty and Professional Services, see:

<http://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

You are entitled to bug fix / maintenance releases for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

<http://eSupport.3com.com/>

To obtain software releases that follow the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

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 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, 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.

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	800 616 1463
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. 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			

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	Luxembourg	800 23625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 4411 357
France	0800 917959	Portugal	800 831416
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.K.	0800 096 3266

Country	Telephone Number	Country	Telephone Number
---------	------------------	---------	------------------

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: warranty_repair@3com.com

Contract requests: emea_contract@3com.com

Latin America - Telephone Technical Support and Repair

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

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

US and Canada — Telephone Technical Support and Repair

All locations:	Network Jacks; Wired or Wireless Network Interface Cards:	1 800 876 3266
	All other 3Com products:	1 800 876 3266

REGULATORY NOTICES

FCC STATEMENT

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

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

ICES STATEMENT

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

CE STATEMENT (EUROPE)

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

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

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

A copy of the signed Declaration of Conformity can be downloaded from the Product Support web page for the Baseline Switch 2948-SFP Plus at <http://www.3Com.com>.

Also available at http://support.3com/doc/BL_WEITCH_2948_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A情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。