

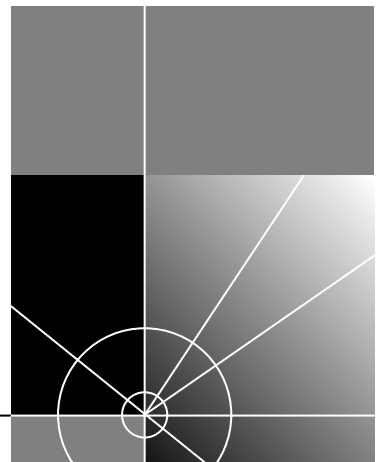


# SuperStack® II Switch 9000 SX User Guide

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

Part No. DUA1699-0AAA02  
100001-00 Rev. 02  
Published April 1998

---



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

Copyright © **3Com Corporation, 1998**. 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 permission from 3Com Technologies.

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

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

**UNITED STATES GOVERNMENT LEGENDS:**

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

**For units of the Department of Defense:**

*Restricted Rights Legend:* Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for Restricted Rights in Technical Data and Computer Software Clause at 48 C.F.R. 52.227-7013. 3Com Technologies, c/o 3Com Limited, 3Com Centre, Boundary Way, Hemel Hempstead, Herts, HP2 7YU, United Kingdom.

**For civilian agencies:**

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 Unpublished rights reserved under the copyright laws of the United States.

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. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

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

3Com, EtherLink, SuperStack, and Transcend are registered trademarks of 3Com Corporation and 3TECH is a trademark of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

## **Electromagnetic Compatibility**

---

### **FCC Statement**

This equipment has been tested with a class A computing device and has been found to comply with part 15 of FCC Rules. Operation in a residential area may cause unacceptable interference to radio and TV receptions, requiring the operator to take whatever steps are necessary to correct the interference.

---

### **CSA Statement**

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

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

---

## VCCI Statement

### VCCI Class 2 ステートメント

この装置は、第二種情報装置(住宅地域又はその隣接した地域において使用されるべき情報装置)で住宅地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。しかし、本装置をラジオ、テレビジョン受信機に隣接してご使用になると、受信障害の原因となることがあります。取扱説明書に従って正しい取り扱いをして下さい。

---

## 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.



# CONTENTS

---

## ABOUT THIS GUIDE

Introduction	1
Terminology	1
Finding Information in This Guide	2
Conventions	3
Command Syntax Symbols	4
Line-Editing Commands	5
Related Publications	5

---

## 1 SWITCH 9000 OVERVIEW

About the Switch 9000	1-1
Summary of Features	1-1
Port Connections	1-2
Full Duplex	1-3
Switch Operation	1-3
Virtual LANs (VLANs)	1-3
Priority Access Control Enabled (PACE)	1-3
Spanning Tree Protocol (STP)	1-3
IP Unicast Routing	1-4
Network Configuration Example	1-4
Switch 9000 Front View	1-6
Ports	1-6
LEDs	1-7
Switch 9000 Rear View	1-8
Power Socket	1-8
Serial Number	1-8
MAC Address	1-8
Console Port	1-8
Factory Defaults	1-9

---

## 2 INSTALLATION AND SETUP

- Following Safety Information 2-1
- Determining the Switch 9000 Location 2-1
  - Configuration Rules for Gigabit Ethernet 2-2
- Installing the Switch 9000 2-2
  - Rack Mounting 2-2
  - Free-Standing 2-3
  - Stacking the Switch and Other Devices 2-4
- Connecting Equipment to the Console Port 2-4
- Powering-up the Switch 2-6
- Checking the Installation 2-6
  - Power On Self-Test (POST) 2-6
- Logging on for the First Time 2-6

---

## 3 ACCESSING THE SWITCH

- Security Access Levels 3-1
  - User Access Level 3-1
  - Administrator Access Level 3-2
  - Default Accounts 3-2
    - Adding a Password to the Default *admin* Account 3-2
  - Creating a Management Account 3-3
    - Changing Account Passwords 3-3
    - Viewing Switch Accounts 3-4
    - Deleting a Switch Account 3-4
- Methods of Managing the Switch 9000 3-4
  - Using the Console Interface 3-5
- Using Telnet 3-5
  - Configuring Switch IP Parameters 3-5
    - Using a BOOTP Server 3-5
    - Manually Configuring the IP Settings 3-6
  - Disconnecting a Telnet Session 3-7
  - Disabling Telnet Access 3-8
- Using SNMP 3-8
  - Accessing Switch Agents 3-9
  - Saving Configuration Changes 3-9
  - Supported MIBs 3-9
  - Supported Traps 3-9

Configuring SNMP Settings	3-10
Displaying SNMP Settings	3-11
Resetting and Disabling SNMP	3-12
Checking Basic Connectivity	3-12
Ping	3-12
Traceroute	3-13
Configuring Ports	3-13
Enabling and Disabling Ports	3-13
Configuring Autonegotiation	3-13
Port Commands	3-14
Load Sharing	3-14
Configuring Load Sharing	3-15
Verifying the Load Sharing Configuration	3-16
Current Limitations of Load Sharing	3-16

---

## 4 COMMANDS

Understanding the Command Syntax	4-1
Syntax Helper	4-2
Command Completion	4-2
Abbreviated Syntax	4-2
Command Shortcuts	4-2
Numerical Ranges	4-3
Names	4-3
Symbols	4-3
Line-Editing Commands	4-4
Command History Substitution	4-5
Common Commands	4-5
Switch 9000 Commands	4-6
General Switch Commands	4-7
User Account Commands	4-8
Switch Management Commands	4-9
VLAN Commands	4-10
Protocol Commands	4-11
FDB Commands	4-11
Port Commands	4-12
PACE Commands	4-13
STP Commands	4-13

Basic IP Commands	4-15
IP ARP Commands	4-16
IP Route Table Commands	4-17
ICMP Commands	4-17
4-18	
RIP Commands	4-19
4-20	
Logging Commands	4-21
4-22	
Configuration and Image Commands	4-23

---

## **5 VIRTUAL LANS (VLANs)**

Overview of Virtual LANs	5-1
Benefits	5-1
Types of VLANs	5-2
Port-Based VLANs	5-2
Expanding Port-Based VLANs Across Switches	5-4
Tagged VLANs	5-6
Uses of Tagged VLANs	5-6
Assigning a VLAN Tag	5-6
Mixing Port-based and Tagged VLANs	5-8
Protocol-based VLANs	5-8
Predefined Protocol Filters	5-9
Defining Protocol Filters	5-10
VLAN Names	5-10
The Default VLAN	5-11
Configuring VLANs on the Switch 9000	5-11
VLAN Configuration Examples	5-12
Displaying VLAN Settings	5-13
Deleting and Resetting VLANs	5-15

---

## **6 SWITCH FORWARDING DATABASE (FDB)**

Overview of the FDB	6-1
FDB Contents	6-1
FDB Entry Types	6-1
PACE Prioritization	6-2
How FDB Entries are Added	6-2



Configuring FDB Entries	6-3
FDB Configuration Example	6-3
Displaying FDB Entries	6-3
Removing FDB Entries	6-4

---

## **7 SPANNING TREE PROTOCOL (STP)**

Overview of the Spanning Tree Protocol	7-1
How STP Works	7-3
Initialization	7-3
Stabilization	7-4
Reconfiguration	7-4
Spanning Tree Domains	7-4
Defaults	7-5
STP Configurations	7-6
STP Configurations to Avoid	7-8
Creating STP Domains	7-9
Enabling STP on the Switch	7-10
Configuring STP	7-10
Configuration Example	7-12
Displaying STP Settings	7-12
Disabling and Resetting STP	7-14

---

## **8 IP UNICAST ROUTING**

Overview of IP Unicast Routing	8-1
Router Interfaces	8-1
Populating the Routing Table	8-2
Dynamic Routes	8-3
Static Routes	8-3
Multiple Routes	8-3
Configuring IP Unicast Routing	8-4
Verifying the IP Unicast Routing Configuration	8-5
Configuring DHCP/BOOTP Relay	8-5
Verifying the DHCP/BOOTP Relay Configuration	8-5
Routing Configuration Example	8-10
Displaying Router Settings	8-12
Resetting and Disabling Router Settings	8-13

---

## **9 STATUS MONITORING AND STATISTICS**

- Status Monitoring 9-1
- Port Statistics 9-4
- Port Errors 9-6
- Switch Logging 9-7
  - Local Logging 9-8
    - Real-time Display 9-8
  - Remote Logging 9-9
  - Logging Commands 9-10
- RMON 9-11
  - About RMON 9-11
  - About the RMON Groups 9-12
    - Statistics 9-12
    - History 9-12
    - Alarms 9-13
    - Events 9-13
  - Benefits of RMON 9-13
    - Improving Efficiency 9-13
    - Allowing Proactive Management 9-13
    - Reducing the Traffic Load 9-13
  - RMON and the Switch 9-14
  - RMON Features of the Switch 9-14
  - About Event Actions 9-15

---

## **10 SOFTWARE UPGRADE AND BOOT OPTIONS**

- Upgrading the Software 10-1
  - Rebooting the Switch 10-2
- Saving Configuration Changes 10-2
  - Returning to Factory Defaults 10-3
- Boot Option Commands 10-3

---

## **A SAFETY INFORMATION**

- Important Safety Information A-1
  - Power A-1
  - Power Cord A-2
  - Fuse A-3

Fiber Optic Ports	A-3
Lithium Battery	A-4
L'information de Sécurité Importante	A-4
Power	A-5
Cordon électrique	A-6
Fuse	A-6
Ports pour fibres optiques	A-7
Batterie au lithium	A-7
Wichtige Sicherheitsinformationen	A-8
Power	A-8
Power Cord	A-9
Fuse	A-9
Faseroptikanschlüsse - Optische Sicherheit	A-10
Lithiumbatterie	A-11

---

## **B TECHNICAL SPECIFICATIONS**

---

## **C TROUBLESHOOTING**

LEDs	C-1
Using the Command-Line Interface	C-2
VLANs	C-4
STP	C-5
Routing	C-6

---

## **D TECHNICAL SUPPORT**

Online Technical Services	D-1
World Wide Web Site	D-1
3Com Bulletin Board Service	D-1
Access by Analog Modem	D-1
Access by Digital Modem	D-2
3ComFactsSM Automated Fax Service	D-2
3ComForum on CompuServe® Online Service	D-3
Support from Your Network Supplier	D-3
Support from 3Com	D-4
Returning Products for Repair	D-5

---

**GLOSSARY**

---

**INDEX**

---

**3COM CORPORATION LIMITED WARRANTY**

# ABOUT THIS GUIDE

*About This Guide* provides an overview of this guide, describes guide conventions, tells you where to look for specific information and lists other publications that may be useful.

---

## Introduction

This guide provides the required information to install and configure the Superstack® II Switch 9000 SX (3C16990).

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of:

- *Local Area Networks (LANs)*
- Ethernet concepts
- Ethernet switching and bridging concepts
- *Simple Network Management Protocol (SNMP)*
- IP Routing



*The Release Notes shipped with the Switch 9000 may contain information that updates or overrides information in this guide. You should always follow the information in the Release Notes if it is different from the information given in this guide.*

## Terminology

Throughout this guide, the term Switch 9000 is used to refer to the SuperStack II Switch 9000 SX.

For definitions of other terms used in this guide, refer to the "Glossary," located at the end of the user guide.

The terms Forwarding Database and Switch Database are interchangeable.

## Finding Information in This Guide




This table shows where to find specific information in this guide.

<b>Task</b>	<b>Location</b>
Learning concepts	Chapter 1, "Switch 9000 Overview"
Installing the Switch 9000	Chapter 2, "Installation and Setup" Appendix A, "Safety Information"
Setting up user accounts	Chapter 3, "Accessing The Switch"
Understanding the Command-Line Interface	Chapter 4, "Commands"
Creating a VLAN	Chapter 5, "Virtual LANs (VLANs)"
Understanding the Switch Forwarding Database (FDB)	Chapter 6, "Switch Forwarding Database (FDB)"
Configuring Spanning Tree Protocol parameters	Chapter 7, "Spanning Tree Protocol (STP)"
Configuring IP Unicast Routing	Chapter 8, "IP Unicast Routing"
Monitoring	Chapter 9, "Status Monitoring and Statistics"
Saving the Switch configuration	Chapter 10, "Software Upgrade and Boot Options"
Upgrading the Switch software	Chapter 10, "Software Upgrade and Boot Options"
Technical Specifications	Appendix B, "Technical Specifications"
Troubleshooting	Appendix C, "Troubleshooting"
Getting technical support	Appendix D, "Technical Support"
Identifying terms	"Glossary"

## Conventions

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

**Table 1** Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

**Table 2** Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names appear in text in one of two ways: <ul style="list-style-type: none"> <li>■ Referred to by their labels, such as "the Return key" or "the Escape key"</li> <li>■ Written with brackets, such as [Return] or [Esc]</li> </ul> If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in <b>boldface</b> type	Bold text denotes key features.

## Command Syntax Symbols

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table 3 summarizes command syntax symbols.

**Table 3** Command Syntax Symbols

Symbol	Description
angle brackets < >	<p>Enclose a variable or value. You must specify the variable or value. For example, in the syntax</p> <pre>config vlan &lt;name&gt; ipaddress &lt;ip_address&gt;</pre> <p>you must supply a VLAN name for &lt;name&gt; and an address for &lt;ip_address&gt; when entering the command. Do not type the angle brackets.</p>
square brackets [ ]	<p>Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>disable vlan [&lt;name&gt;   all]</pre> <p>you must specify either the VLAN name for &lt;name&gt;, or the keyword "all" when entering the command. Do not type the square brackets.</p>
vertical bar	<p>Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax</p> <pre>config snmp community [read   write] &lt;string&gt;</pre> <p>you must specify either the read or write community string in the command. Do not type the vertical bar.</p>
braces { }	<p>Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>show vlan {&lt;name&gt;   all}</pre> <p>you can specify either a particular VLAN or the keyword "all." If you do not specify an argument, the command will show all VLANs. Do not type the braces.</p>



---

**Line-Editing Commands**

Table 4 describes the line-editing commands available using the command-line interface.

**Table 4** Line-Editing Commands

Command	Description
Backspace	Deletes character to the left of cursor and shifts remainder of line to left.
Delete or [Ctrl] + D	Deletes character under cursor and shifts remainder of line to left.
[Ctrl] + K	Deletes characters from under cursor to the end of the line.
Insert	Toggles on and off. When toggled on, inserts text and pushes previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [Ctrl]+A	Moves cursor to first character in line.
End or [Ctrl]+E	Moves cursor to last character in line.
[Ctrl]+L	Clears the screen and moves the cursor to the beginning of the line.
Up Arrow	Displays the previous command in the command history buffer, and places cursor at end of command.
Down Arrow	Displays the next command in the command history buffer, and places cursor at end of command.

---

The command syntax is explained in Chapter 4.

---

**Related Publications**

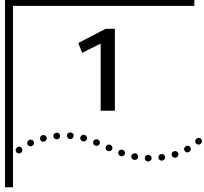
The Switch 9000 documentation set includes the following:

- SuperStack II Switch 9000 SX Quick Reference Guide. Part Number DQA1699-OAAA03.
- SuperStack II Switch 9000 SX Quick Installation Guide. Part Number DIA1699-OAAA02.
- SuperStack II Switch 9000 SX Release Note. Part Number DNA1699-OAAA03.

3Com's home page can be found at the following web site:

- <http://www.3com.com/>





# SWITCH 9000 OVERVIEW

This chapter describes the following:

- Switch 9000 features
- How to use the Switch 9000 in your network configuration
- Switch 9000 front view
- Switch 9000 rear view
- Factory default settings

---

## About the Switch 9000

Network managers are currently faced with the challenge of creating networks that can provide high-speed and high performance to serve the needs of today's network users.

Part of the 3Com SuperStack® II range of products, the Switch 9000 provides switching between multiple Gigabit Ethernet ports.

---

## Summary of Features

The Switch 9000 has the following features:

- Eight Gigabit Ethernet ports
- Support for 12,000 addresses in the Switch forwarding database
- Fully nonblocking operation
  - All ports transmit and receive packets at wire speed
- Full duplex operation
- 4Mb packet memory

- *Virtual LANs (VLANs)*
  - Support for 64 VLANs on a single Switch 9000
  - Support for IEEE 802.1Q tagging
  - Controls traffic (including broadcasts)
  - Provides extra security
  - Protocol-sensitive filtering for VLANs
- Recognition of *the Priority Access Control Enabled (PACE)* bit set by 3Com Etherlink<sup>®</sup> adapters and the other devices that support PACE
- Responds to 802.3x flow-control messages
- Auto-negotiation to IEEE 802.3z for plug and play
- Load sharing
- *Spanning Tree Protocol (IEEE 802.1d)*
- Multiple spanning trees (64)
- Wirespeed *Internet Protocol (IP)* via *Routing Information Protocol (RIP)* version 1 and RIP version 2
- Wirespeed *Internet Protocol (IP)* unicast routing
- 3Com's SuperStack<sup>®</sup> II architecture
  - Integrated network management
  - 19-inch rack or free-standing mounting
- Agent support
  - *Simple Network Management Protocol (SNMP)*
  - *Remote Monitoring (RMON)* groups 1 to 4 — statistics, history, alarms, and events
  - Repeater and Bridge *Management Information Base (MIB)*
  - Easy software upgrades
  - BOOTP for automatic *Internet Protocol (IP)* address configuration
  - Local management

### Port Connections

The Switch 9000 provides eight 850nm fiber-optic Gigabit Ethernet ports, using duplex SC connectors. Using the eight ports, you can connect other Gigabit Ethernet devices (such as 10/100 switches that have Gigabit Ethernet modules) to the Switch 9000. You can also connect Switch 9000 devices to each other.

**Full Duplex** The Switch 9000 provides full-duplex support for all ports. Full-duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a link. The Switch 9000 will refuse a half duplex connection on any port.

**Switch Operation** The Switch 9000 uses the same algorithm as a conventional 802.1d bridge for filtering, forwarding, and learning packets.

### Virtual LANs (VLANs)

The Switch 9000 has a *Virtual LAN (VLAN)* feature that allows you to build your network segments without being restricted by physical connections. A VLAN is a group of location- and topology-independent devices that communicate as if they are on the same physical *Local Area Network (LAN)*. Implementing VLANs on your network has the following three advantages:

- It eases the change and movement of devices on networks. If a device in VLAN *marketing* is moved to a port in another part of the network, all you must do is specify that the new port belongs to VLAN *marketing*.
- It helps to control broadcast traffic. If a device in VLAN *marketing* transmits a broadcast frame, only VLAN *marketing* devices receive the frame.
- It provides extra security. Devices in VLAN *marketing* can only communicate with devices on VLAN *sales* using a device that provides routing services.



*For more information on VLANs, refer to Chapter 5.*

### Priority Access Control Enabled (PACE)

The Switch recognizes the PACE bit set by 3Com Etherlink® adapters and other devices supporting PACE. When enabled, traffic with these bits receives priority service from the Switch.

### Spanning Tree Protocol (STP)

The Switch 9000 supports the IEEE 802.1d *Spanning Tree Protocol (STP)* which is a bridge-based mechanism for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure the following:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.



*For more information on STP, refer to Chapter 7.*

### **IP Unicast Routing**

The Switch 9000 can route IP traffic between the VLANs configured as virtual router interfaces. Both dynamic and static IP routes are maintained in the routing table. RIP version 1 and RIP version 2 are supported.

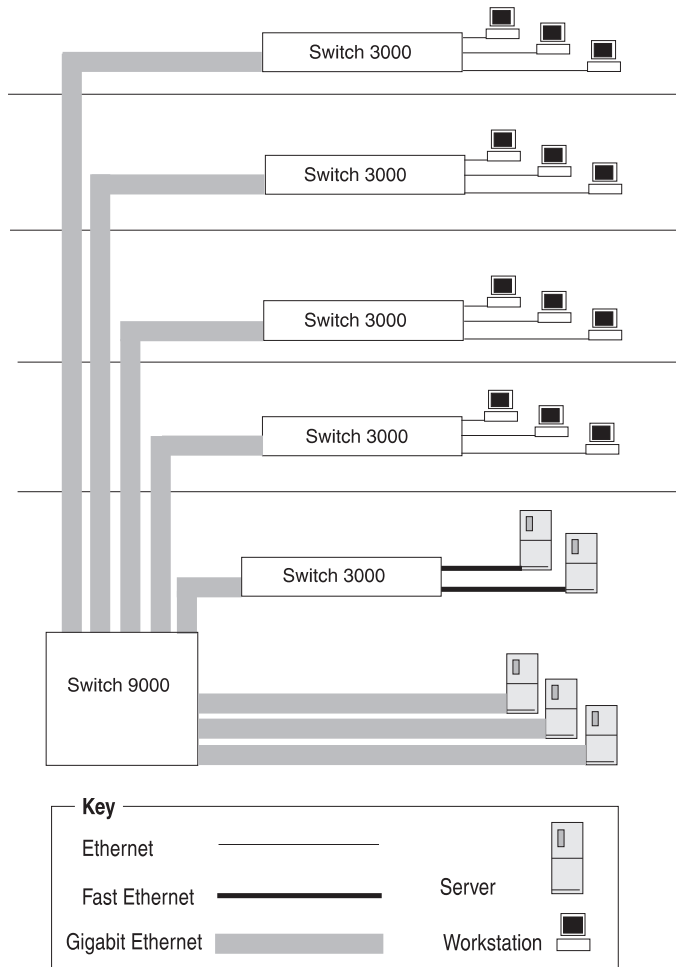


*For more information on IP unicast routing, refer to Chapter 8.*

---

## **Network Configuration Example**

This section describes where to position the Switch 9000 within your network. One common use of the Switch 9000 is on a Gigabit Ethernet backbone. Figure 1-1 shows an example of a Gigabit Ethernet backbone within a building.



**Figure 1-1** Switch 9000 used in a backbone configuration

The Switch 3000 on each floor is provided with a Gigabit Ethernet full-duplex link to the Switch 9000.

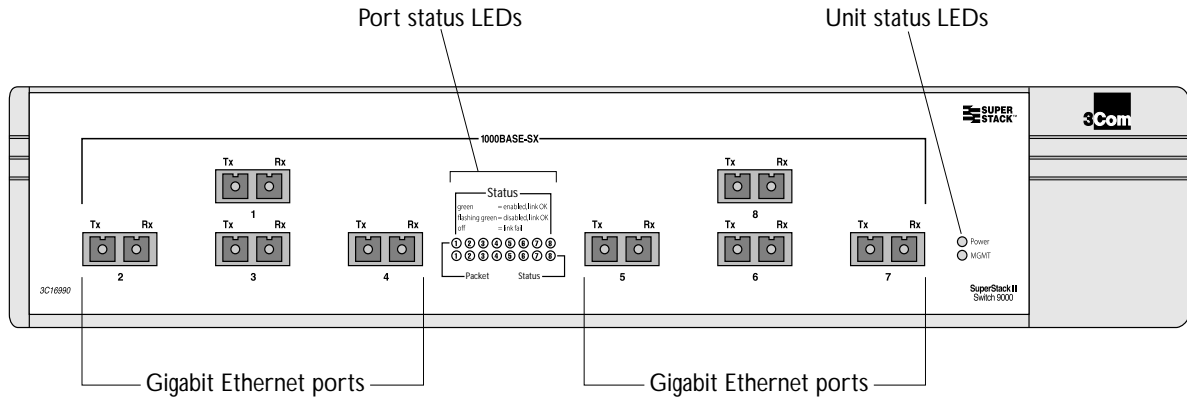
Using Gigabit Ethernet as a backbone technology removes bottlenecks by providing scalable bandwidth, low-latency, high-speed data switching.

In addition to providing a fast backbone between Ethernet LANs, Gigabit Ethernet equipped file servers and services may be directly

attached to the Switch 9000 providing improved performance to the Ethernet desktop.

## Switch 9000 Front View

Figure 1-2 shows the Switch 9000 front view.



**Figure 1-2** Switch 9000 front view

The front panel has the following features:

### Ports

The Switch 9000 has eight 850 nanometer fiber-optic Gigabit Ethernet ports. All use SC connectors and support 62.5/125 micron or 50/125 micron fiber-optic cable. The Switch 9000 ports support the media types and distances listed in Table 1-1.

**Table 1-1** Media Types and Distances

		Distance	
		50/125 micron Multimode Fiber	62.5/125 micron Multimode Fiber
Gigabit Type	850nm Multimode Optics	550 meters	260 meters



For more information on 1000Base-SX and 1000Base-LX link characteristics, refer to IEEE Draft P802.3z/D3.1, Table 38-8.



## LEDs

Table 1-2 describes the LED behavior on the Switch 9000.

**Table 1-2** Switch 9000 LEDs

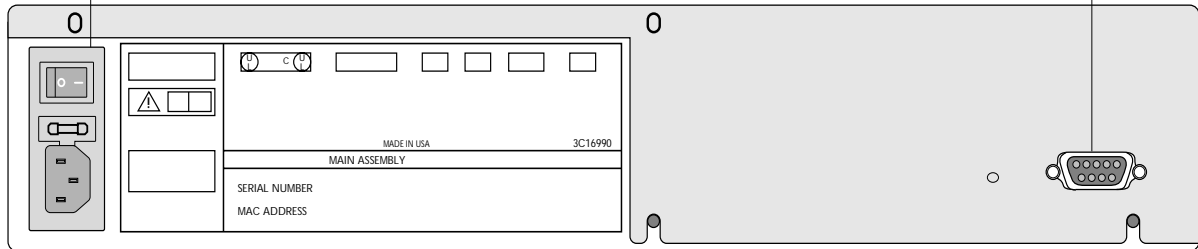
LED	Color	Indicates
<b>Port Status LEDs</b>		
Packet	Yellow	Frames are being transmitted/received on this port.
	Off	No activity on this port.
Status	Green	Link is present; port is enabled.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.
<b>Unit Status LEDs</b>		
Power	Green	The Switch 9000 has been started up.
MGMT	Green	The Switch 9000 is operating normally.
	Green flashing	Software download is in progress.
		Power On Self Test (POST) is in progress.
	Yellow	The Switch 9000 has failed its POST, or is indicating an overheat condition.

## Switch 9000 Rear View

Figure 1-3 shows the Switch 9000 rear view.

Power socket and fuse

Console port



**Figure 1-3** Switch 9000 rear view

The rear panel has the following features:

### Power Socket

The Switch 9000 automatically adjusts to the supply voltage. The power supply operates down to 90 V. The fuse is suitable for both 110 V AC and 220-240 V AC operation.

### Serial Number

The serial number uniquely identifies this unit. You may need this serial number for fault-reporting purposes.

### MAC Address

This label shows the unique Ethernet MAC address assigned to this device.

### Console Port

The console port (9-pin, "D" type connector) is used to connect a terminal and to carry out local out-of-band management.

## Factory Defaults

Table 1-3 shows the factory defaults for the Switch 9000 features.

**Table 1-3** Switch 9000 Factory Defaults

Item	Default Setting
Port status	Enabled on all ports
Default user account	<i>admin</i> with no password and <i>user</i> with no password
Console port configuration	9600 baud, eight data bits, one stop bit, no parity, XON/XOFF flow control enabled
SNMP read community string	Public
SNMP write community string	Private
RMON history session	Enabled
RMON alarms	Enabled <ul style="list-style-type: none"> <li>■ Send trap if load is greater than 75% of available bandwidth</li> <li>■ Send trap if there are more than 10 errors in 1,000 packets</li> </ul>
PACE	Recognition disabled
Virtual LANs	One VLAN named <i>default</i> ; all ports belong to the default VLAN; no protocol filter used.
802.1Q tagging	All packets are untagged on the default VLAN ( <i>default</i> )
BOOTP	Enabled on the default VLAN ( <i>default</i> )
Spanning Tree Protocol	Disabled; one defined as "s0"
IP Routing	Disabled
Forwarding database aging period	30 minutes
Auto-negotiation	On



# 2

## INSTALLATION AND SETUP

This chapter describes the following:

- How to decide where to install the Switch 9000
- Gigabit Ethernet configuration rules
- How to install the Switch in a rack or free-standing
- How to connect equipment to the console port
- How to check the installation using the *Power On Self-Test (POST)*

---

### Following Safety Information

Before installing or removing any components of the Switch, or before carrying out any maintenance procedures, you must read the safety information provided in Appendix A of this guide.

---

### Determining the Switch 9000 Location

The Switch 9000 is suited for use in the office, where it can be free-standing or mounted in a standard 19-inch equipment rack. Alternatively, the device can be rack-mounted in a wiring closet or equipment room. Two mounting brackets are supplied with the Switch.



**CAUTION:** *When using a rack mounting system, the Switch must be mounted on a shelf or runners. The rack mounting brackets alone are not sufficient to support the weight of the Switch. The rack mounting brackets are provided to ensure stability across the horizontal plane. If you stack Switches, you must ensure that the shelf or runners are strong enough to hold the combined weight. Ensure that the ventilation holes are not obstructed.*

After deciding where to install the Switch, make sure that:

- You will be able to meet the configuration rules detailed in Chapter 1.
- The Switch is accessible and cables can be connected easily.

- Water or moisture cannot enter the case of the unit.
- Temperature must be within the range of 0 to 40 degrees Celsius.
- Air-flow around the unit and through the vents in the side of the case is not restricted. You should provide a minimum of 25mm (1-inch) clearance.
- No objects are placed on top of the unit.
- Units are not stacked more than four high if the Switch is free-standing.

### Configuration Rules for Gigabit Ethernet

The connectors, supported media types, and maximum distances for the Switch 9000 are described in Chapter 1.

---

### Installing the Switch 9000

The Switch 9000 can be mounted in a rack, or placed free-standing on a tabletop.

#### Rack Mounting

The Switch 9000 is 2U high and will fit in most standard 19-inch racks.

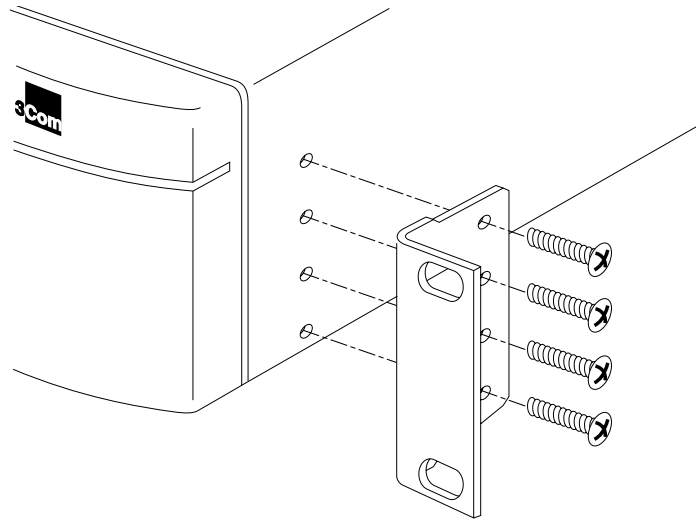
The Switch should only be used in a rack if it is mounted on runners, a shelf, or a tray to support the weight. The rack mount kits alone are not sufficient to support the weight of the Switch.



**CAUTION:** *The rack mount kits must not be used to suspend the Switch from under a table or desk, or attach it to a wall.*

To install the mounting brackets on the Switch, follow these steps:

- 1 Place the Switch the right way up on a hard flat surface, with the front facing toward you.
- 2 Remove the existing screws from the sides of the chassis.
- 3 Locate a mounting bracket over the mounting holes on one side of the unit.
- 4 Insert the four screws and fully tighten with a suitable screwdriver, as shown in Figure 2-1.



**Figure 2-1** Fitting the mounting bracket

- 5 Repeat the three previous steps for the other side of the Switch.
- 6 Refer to the instructions that shipped with your rack, runners, shelf or tray to complete the installation of the Switch into the mounting rack.



**CAUTION:** When using rack mounting runners, a shelf, or a tray, make sure that the ventilation holes on the side of the Switch are not obstructed.

- 7 Connect cables.

**Free-Standing** The Switch 9000 is supplied with four self-adhesive rubber pads. Apply the pads to the underside of the device by sticking a pad in the marked area at each corner of the Switch.

## Stacking the Switch and Other Devices

Up to four units can be placed on top of one another. If mixing Switch 9000, Switch 3000 FX, Switch 1000, Switch 1200, and other SuperStack® II hubs, the smaller units must be positioned at the top using rubber feet.



*This section relates only to physically placing the devices on top of each other. The Switch cannot be used to form a stack. It cannot be linked to other switches using special expansion cables to form a larger Switch.*

Apply the pads to the underside of the device by sticking a pad in the marked area at each corner of the Switch. Place the devices on top of each other, ensuring that the pads of the upper device line up with the recesses of the lower device.

---

## Connecting Equipment to the Console Port

Connection to the console port is used for direct local management. The Switch 9000 console port settings are set as follows:

- **Baud rate** — 9600
- **Data bits** — 8
- **Stop bit** — 1
- **Parity** — None
- **Flow control** — XON/XOFF

The terminal connected to the console port on the Switch must be configured with the same settings. This procedure will be described in the documentation supplied with the terminal.

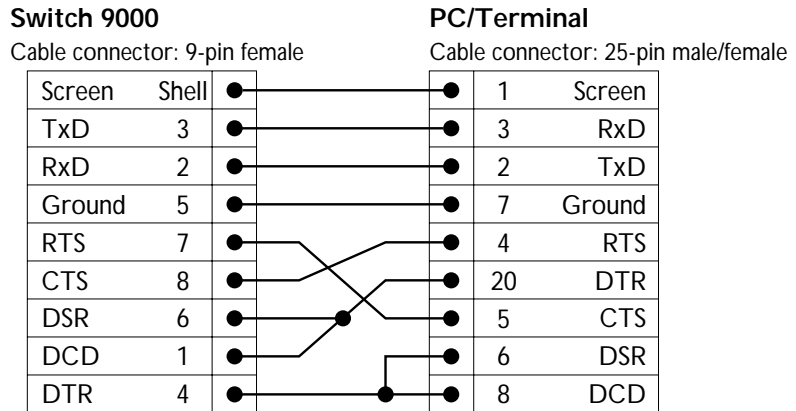
Appropriate cables are available from your local supplier. If you make your own cables, pin-outs for a DB-9 male console connector are described in Table 2-1.

**Table 2-1** Console Connector Pin-Outs

Function	Pin Number
TXD (transmit data)	3
RXD (receive data)	2
GND (ground)	5

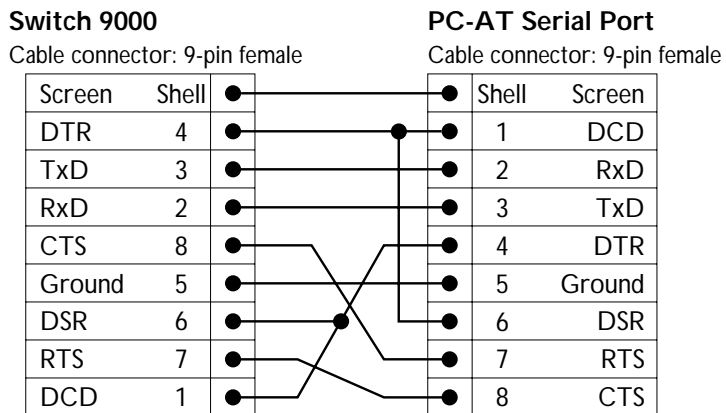


Figure 2-2 shows the pin-outs for a 9-pin to RS-232 25-pin null modem cable.



**Figure 2-2** Null modem cable pin-outs

Figure 2-3 shows the pin-outs for a 9-pin to 9-pin PC-AT serial null modem cable.



**Figure 2-3** PC-AT serial cable pin-outs

---

## Powering-up the Switch

To power-up the Switch, follow these steps:

- 1 Connect the power cable to the Switch.
- 2 Connect the power cable to the wall outlet
- 3 Turn the on/off Switch to the on position.

---

## Checking the Installation

After turning on power to the Switch 9000, the device performs a Power On Self-Test (POST).

### Power On Self-Test (POST)

During the POST, all ports are temporarily disabled, the packet LED is off, the power LED is on, and the MGMT LED flashes green. The MGMT LED flashes until the Switch has successfully passed the POST.

If the Switch passes the POST, the MGMT LED stops blinking and remains green. If the Switch fails the POST, the MGMT LED shows a solid yellow light.

---

## Logging on for the First Time

After the Switch has completed the POST, it is operational. Once operational, you can log on to the Switch and configure an IP address for the default VLAN (named *default*).

To manually configure the IP settings, perform the following steps:

- 1 Connect a terminal or workstation running terminal emulation software to the console port.
- 2 At your terminal, press [Return] until you see the logon prompt.
- 3 At the logon prompt, enter the default user name *admin* to log on with administrator privileges. For example:

```
login: admin
```

Administrator capabilities allow you to access all Switch functions. For more information on Switch security, refer to Chapter 3.

- 4 At the password prompt, press [Return].

The default name, *admin*, has no password assigned. When you have successfully logged on to the Switch, the command-line prompt displays the name of the Switch in its prompt.

- 5 Assign an IP address and subnetwork mask for VLAN *default*. The example below assigns an IP address of 123.45.67.8 and a subnetwork mask of 255.255.255.0.

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
```

Your changes take effect immediately.

- 6 Save your configuration changes so that they will be in effect after the next Switch reboot, by typing

```
save
```



*For more information on saving configuration changes, refer to Chapter 10.*

- 7 When you are finished using the facility, logout of the Switch by typing

```
logout
```



# 3

## ACCESSING THE SWITCH

This chapter describes the following information that you can use to begin managing the Switch 9000:

- Security access level overview
- Configuring the Switch for management
- Switch management methods
- Configuring SNMP



**CAUTION:** *In order for configuration changes to be retained through a Switch power cycle or reboot, you must issue a SAVE command after you have made the change. For more information on the SAVE command, refer to Chapter 10.*

---

### Security Access Levels

The Switch 9000 supports two security access levels:

- User
- Administrator

### User Access Level

A user-level account can view all manageable parameters, with the following exceptions:

- User account information
- SNMP community strings

A user-level account can use the ping command to test device connectivity. A user-level account can also change the password assigned to the account name. If you have logged on with a user access level, the command-line prompt ends with a (>) sign. For example:

```
3C16990>
```

## Administrator Access Level

An administrator-level account can view and change all Switch parameters, add and delete users, and change the password associated with any account name. The administrator can disconnect a Telnet management session. If this happens, the user is notified that the session has been terminated.

If you have logged on with administrator access level, the command-line prompt ends with a (#) sign. For example:

```
3C16990#
```

If an asterisk (\*) appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For example:

```
*3C16990#
```

## Default Accounts

By default, the Switch is configured with two accounts, as shown in Table 3-1.

**Table 3-1** Default Accounts

User Name	Access Level
admin	This user can access and change all manageable parameters. The admin account cannot be deleted.
user	This user can view (but not change) all manageable parameters, with the following exceptions: <ul style="list-style-type: none"> <li>■ This user cannot view the user account database.</li> <li>■ This user cannot view the SNMP community strings.</li> </ul> This user has access to the ping command.

The default accounts do not have passwords assigned to them. Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.

### Adding a Password to the Default *admin* Account

To add a password to the default *admin* account, follow these steps:

- 1 Logon to the Switch using the name *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a default admin password by typing the following:

```
config account admin
```

- 4 Enter the new password at the prompt.
- 5 Re-enter the new password at the prompt.
- 6 Save your changes by typing

**save**

### Creating a Management Account

The Switch can have a total of three management accounts. You can use the default names (admin and user), or you can create new names and passwords for the accounts. Passwords must have a minimum of four characters and can have a maximum of 12 characters.



*The account name "admin" cannot be deleted.*

To create a new account, follow these steps:

- 1 Logon to the Switch using the name *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a new user by typing the following:

```
create account [admin | user] <username>
```

- 4 Enter the password at the prompt.
- 5 Re-enter the password at the prompt.
- 6 Save your changes by typing

**save**

### Changing Account Passwords

To add a password to a user account, follow these steps:

- 1 At the logon prompt, enter your user name and password. Note that they are both case-sensitive. Ensure that you have entered a user name and password with administrator privileges.
  - If you are logging on for the first time, use the default user name *admin* to log on with administrator privileges. For example:

```
login: admin
```

- 2 Add an account password by using the following command:

```
config account <name>
```

for example:

```
config account user
```

- 3 Enter the new password at the prompt.
- 4 Re-enter the new password at the prompt.
- 5 Save your changes by typing

**save**



*If you forget your password contact your local technical support representative, who will advise on your next course of action.*

### Viewing Switch Accounts

To view the accounts that have been created, you must have administrator privileges. Type the following to see the accounts:

**show accounts**

Output from the show accounts command is displayed below.

```
#show accounts
```

User Name	Access	LoginOK	Failed	Session
admin	R/W	0	0	
user	RO	0	0	

### Deleting a Switch Account

To delete a switch account, you must have administrator privileges. Use the following command to delete an account:

```
delete account <username>
```

---

## Methods of Managing the Switch 9000

You can manage the Switch 9000 using the following methods:

- Access the command-line interface by connecting a terminal (or workstation with terminal emulation software) to the Switch 9000 console port.
- Access the command-line interface over a TCP/IP network using a Telnet connection.
- Use an SNMP Network Manager over a network running the IP protocol.

The Switch can support up to four user sessions concurrently (for example, one console port and three Telnet connections).



## Using the Console Interface

The command-line interface built into the Switch is accessible by way of the 9-pin, RS-232 console port located on the rear of the unit.



*For more information on the console port pin-outs, refer to Chapter 2.*

Once the connection is established, you will see the system prompt and you may log on.

---

## Using Telnet

Any Telnet facility should be able to communicate with the Switch over a TCP/IP network. Up to three active Telnet sessions can access the Switch concurrently. The Telnet connection will time out after three minutes of inactivity. If a connection to a Telnet session is lost inadvertently, the Switch will terminate the session within three minutes.

Before you can start a Telnet session you must set up the IP parameters described in “Configuring Switch IP Parameters” on page 3-5. Telnet is enabled by default.

To open the Telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the Telnet client you are using, if you are unsure of how to do this.

Once the connection is established, you will see the system prompt and you may log on.

## Configuring Switch IP Parameters

In order to manage the Switch by way of a Telnet connection or by using an SNMP Network Manager, you must configure the Switch IP parameters. Switch IP parameters are configured on a per-VLAN basis.

### Using a BOOTP Server

If you are using IP and you have a BOOTP server set up correctly on your network, you will need to add the Switch Media Access Control (MAC) address, the IP address, subnetwork mask, and default gateway to the BOOTP server. The Switch MAC address is shown on the rear label of the Switch.

Once this is done, the IP address, subnetwork mask, and default gateway for the Switch will be downloaded automatically. You can then start managing the Switch without further configuration.

You can enable BOOTP on a per-VLAN basis by using the following command:

```
enable bootp vlan [<name> | all]
```

### Manually Configuring the IP Settings

If you are using IP without a BOOTP server, you must enter the IP parameters for the Switch in order for the SNMP Network Manager or Telnet software to communicate with the device. To assign IP parameters to the Switch, you must do the following:

- Logon to the Switch with administrator access level.
- Assign an IP address and subnetwork mask to a VLAN.

The Switch comes configured with a default VLAN named *default*. In order to use Telnet or an SNMP Network Manager, you must have at least one VLAN on the Switch, and it must be assigned an IP address and subnetwork mask. IP addresses are always assigned to a VLAN. The Switch 9000 can be assigned multiple IP addresses. For information on creating and configuring VLANs, refer to Chapter 5, “Virtual LANs (VLANs).”

To manually configure the IP settings, perform the following steps:

- 1 Connect a terminal or workstation running terminal emulation software to the console port.
- 2 At your terminal, press [Return] one or more times until you see the logon prompt.
- 3 At the logon prompt, enter your user name and password. Note that they are both case-sensitive. Ensure that you have entered a user name and password with administrator privileges.

- If you are logging on for the first time, use the default user name *admin* to log on with administrator privileges. For example:

```
login: admin
```

The administrator access level allow you to access all Switch functions. The default user names have no passwords assigned. For more information on Switch security, refer to “Security Access Levels,” on page 3-1.

- If you have been assigned a user name and password with administrator privileges, enter them at the logon prompt.

- 4 At the password prompt, enter the password and press [Return].  
When you have successfully logged on to the Switch, the command-line prompt displays the name of the Switch in its prompt.
- 5 Assign an IP address and subnet mask for the default VLAN by using the following command

```
config vlan <name> ipaddress <ipaddress> {<subnet_mask>}
```

For example:

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
```

Your changes take effect immediately.

- 6 Configure the default route for the Switch using the following command:

```
config iproute add default <ipaddress> {<metric>}
```

For example:

```
config iproute add default 123.0.0.1 1
```

- 7 Save your configuration changes so that they will be in effect after the next Switch reboot, by typing:

```
save
```



*For more information on saving configuration changes, refer to Chapter 10.*

- 8 When you are finished using the facility, logout of the Switch by typing

```
logout
```

### **Disconnecting a Telnet Session**

For security purposes, an administrator access level account can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated.

To terminate a Telnet session, follow these steps:

- 1 Logon to the Switch with an administrator access level.
- 2 Determine the session number of the session you want to terminate by typing

```
show session
```

Sample output from the show session command is as follows:

```
3C16990:2 # sh sess
# Login Time                User      Type      Location
=====
 0 Tue Mar 10 11:10:53 1998 admin  console  serial
 4 Tue Mar 10 13:11:13 1998 user   telnet   192.207.37.168
```

Terminate the session by typing

```
clear session <session_number>
```

### Disabling Telnet Access

By default, Telnet services are enabled on the Switch. You can choose to disable Telnet. To do so, enter

```
disable telnet
```

To re-enable Telnet on the Switch, at the console port enter

```
enable telnet
```

You must be logged on as an administrator to enable or disable Telnet.

---

## Using SNMP

Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the Switch, provided the Management Information Base (MIB) is installed correctly on the management station.

Each Network Manager provides its own user interface to the management facilities. 3Com's Transcend® range of Network Managers all have facilities for managing the Switch.

The following sections describe how to get started if you want to use an SNMP manager. It assumes you are already familiar with SNMP management. If not, refer to the following publication:

“The Simple Book”  
by Marshall T. Rose  
ISBN 0-13-8121611-9  
Published by Prentice Hall

## Accessing Switch Agents

In order to have access to the SNMP agent residing in the Switch, at least one VLAN on the Switch must have an IP address assigned to it. For more information on assigning an IP address, refer to “Manually Configuring the IP Settings,” on page 3-6.

## Saving Configuration Changes

If you make configuration changes to the Switch using an SNMP manager, you must save the changes so that they are not lost on the next Switch reboot. You can save your changes by using the SNMP save attribute, or by issuing the `save` command from the command line interface.

## Supported MIBs

In addition to private MIBs, the Switch 9000 supports the standard MIBs listed in Table 3-2.

**Table 3-2** Supported MIBs

Description	RFC Number
MIB II	1213
Bridge MIB	1493
RMON	1757
RMON II Probe Configuration	2021
Evolution of Internet	1573

## Supported Traps

A *trap* is a message sent by an SNMP agent to an authorized trap receiver (usually a network management station) to indicate the occurrence of a significant event, such as an error condition or a threshold that has been reached. The Switch 9000 supports the traps listed in Table 3-3.

**Table 3-3** Supported Traps

Trap	Description
Cold start	Indicates that the device is reinitializing itself.
Link up	Indicates that the device recognizes that one of its communication links has come up.
Link down	Indicates that the device recognizes a failure in one of the communication links represented in the agent’s configuration.
Rising alarm	Indicates that an RMON alarm entry has crossed its rising threshold

continued

**Table 3-3** Supported Traps (continued)

Trap	Description
Falling alarm	Indicates that an RMON alarm entry has crossed its falling threshold.
Fan fail	Indicates that one or more of the cooling fans inside the device has failed. A Fan okay trap will be issued once the fan has attained normal operation.
Fan okay	Indicates that a fan has transitioned out of a failure state and is now operating correctly.
Overheat	Indicates that the onboard temperature sensor has reported an overheat condition. The system will shutdown until the device has sufficiently cooled such that operation may begin again. A Cold start trap will be issued when the device comes back on line.
Login attempt failure	Indicates that three consecutive bad logon attempts have occurred.

### Configuring SNMP Settings

The following SNMP parameters can be configured on the Switch:

- **Authorized trap receivers** — An authorized trap receiver can be one or more network management stations on your network. The Switch sends SNMP traps to the trap receiver. You can have a maximum of six trap receivers configured for each Switch 9000.
- **Community strings** — The *community strings* allow a simple method of authentication between the Switch and the remote Network Manager. There are two community strings on the Switch 9000. The read community string provides read-only access to the Switch. The default read community string is *public*. The write community string provides read and write access to the Switch. The default write community string is *private*. The community string for all authorized trap receivers must be configured on the Switch in order for the trap receiver to receive Switch-generated traps.
- **System contact** (optional) — The system contact is a text field that allows you to enter the name of the person(s) responsible for managing the Switch.
- **System name** — The system name is the name that you have assigned to this Switch. The default name is 3C16990.
- **System location** (optional) — Using the system location field, you can enter a location for this Switch.

Table 3-4 describes SNMP configuration commands.

**Table 3-4** SNMP Configuration Commands

Command	Description
config vlan <name> ipaddress <ip_address> {<mask>}	Configures an IP address for the VLAN. This is required in order to use an SNMP manager.
enable snmp access	Allows you to turn on SNMP support for the Switch.
enable snmp trap	Allows you to turn on SNMP trap support.
config snmp add <ipaddress>	Allows you to add the IP address of an SNMP management station to the access list. Up to six address can be specified.
config snmp add trapreceiver <ipaddress> {<string>}	Allows you to add the IP address of a specified trap receiver. A maximum of six trap receivers is allowed.
config snmp community [read   readwrite] <string>	Allows you to configure the SNMP read and write community strings. The community string can have a maximum of 32 characters.
config snmp delete [<ipaddress>   all]	Allows you to delete the IP address of a specified SNMP management station or all SNMP management stations.
config snmp delete trapreceiver [<ip_address>   all]	Allows you to delete the IP address of a specified trap receiver or all authorized trap receivers. If you delete all trap receiver addresses, any machine can have SNMP management access to the Switch.
config snmp syscontact <string>	Allows you to configure the name of the system contact. A maximum of 32 characters is allowed.
config snmp sysname <string>	Allows you to configure the name of the Switch. The sysname appears in the command line interface prompt. A maximum of 32 characters is allowed. The default sysname is 3C16990.
config snmp syslocation <string>	Allows you to configure the location of the Switch. A maximum of 32 characters is allowed.

### Displaying SNMP Settings

To display the SNMP settings configured on the Switch 9000, use the following command:

```
show management
```

This command displays the following information:

- Enable/disable state for telnet, SNMP, and web access
- SNMP community strings

- Authorized SNMP station list
- SNMP trap receiver list
- Logon statistics

### Resetting and Disabling SNMP

To reset or disable SNMP settings, use the commands in Table 3-5.

**Table 3-5** SNMP Reset and Disable Commands

Command	Description
disable snmp access	Allows you to disable SNMP on the Switch.
disable snmp trap	Allows you to prevent SNMP traps from being sent from the Switch.
unconfig management	Restores default values to all SNMP-related entries.

### Checking Basic Connectivity

The Switch 9000 has the following two facilities for checking basic connectivity:

- ping
- traceroute

#### Ping

The ping command allows you to send *Internet Control Message Protocol (ICMP)* echo messages to a remote IP device. The ping command is available for both the user and administrator privilege level.

The ping command syntax is as follows:

```
ping {continuous} {size <n>} <ip_address>
```



Options for the ping command are described in Table 3-6.

**Table 3-6** Ping Command Parameters

Parameter	Description
continuous	Allows you to specify ICMP echo messages to be sent continuously.
size <n>	Allows you to specify the size of the packet.

**Traceroute** The traceroute command allows you to trace the routed path between the Switch and a destination endstation.

The traceroute command syntax is as follows:

```
traceroute <ip_address>
```

where *ip\_address* is the IP address of the destination endstation.

---

**Configuring Ports** Ports on the Switch 9000 can be configured in the following ways:

- Enabling and disabling individual ports
- Configuring autonegotiation
- Creating load-sharing groups on multiple ports

**Enabling and Disabling Ports** By default, all ports are enabled. To enable or disable one or more ports, use the following command:

```
[enable | disable] port <portlist>
```

For example, to disable ports 3, 5, and 6, enter the following:

```
disable port 3,5-6
```

Even though a port is disabled, the link remains enabled for diagnostic purposes.

**Configuring Autonegotiation** By default, the Switch 9000 is configured to use autonegotiation. You can automatically turn autonegotiation on and off.

To turn off autonegotiation, use the following command:

```
config port <portlist> auto off duplex full
```

To configure the Switch to autonegotiate, use the following command:

```
config port <portlist> auto on
```

## Port Commands

Table 3-7 describes port commands.

**Table 3-7** Port Commands

Command	Description
<code>config port &lt;portlist&gt; auto on</code>	Allows you to enable 802.3z autonegotiation.
<code>config port &lt;portlist&gt; auto off duplex full</code>	Allows you to disable autonegotiation on one or more ports.
<code>enable port &lt;portlist&gt;</code>	Allows you to enable one or more ports.
<code>disable port &lt;portlist&gt;</code>	Allows you to disable one or more ports. Even when disabled, the link is available for diagnostic purposes.
<code>show port &lt;portlist&gt; config</code>	Displays state, link status, speed, and autonegotiation setting for each port.
<code>show port &lt;portlist&gt; stats</code>	Displays port information including physical layer configuration and statistics.
<code>show port &lt;portlist&gt; errors</code>	Displays error information for one or more ports.
<code>show port &lt;portlist&gt; collisions</code>	Displays real-time collision statistics.
<code>show port &lt;portlist&gt; packet</code>	Displays a histogram of packet statistics for one or more ports.
<code>show port &lt;portlist&gt; util</code>	Displays port utilization by percentage, bytes per second, or packets per second. Use the space bar to toggle between percentage, bytes per second, or packets per second. Use the clear counters command to reset values.

## Load Sharing

Load sharing with Switch 9000 Switches allows you to increase bandwidth and resilience by using a group of ports to carry traffic in parallel between Switches. The sharing algorithm allows the Switch to use multiple ports as a single logical port. For example, VLANs see the load-sharing group as a single virtual port. The algorithm also guarantees packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

Load sharing is most useful in cases where the traffic transmitted from the Switch to the load-sharing group is sourced from an equal or greater number of ports on the Switch. For example, traffic transmitted to a 2-port load-sharing group should originate from a minimum of two other ports on the same Switch.

This feature is supported between Switch 9000 Switches only, but may be compatible with third-party “trunking” or sharing algorithms.

### Configuring Load Sharing

To set up the Switch 9000 to load share among ports, you must create a load-sharing group of ports. Load-sharing groups are defined according to the following rules:

- Ports on the Switch are divided into groups of two or four.
- Ports in a load-sharing group must be contiguous.
- Valid port combinations are distinguished by the outlined boxes in Table 3-8.
- The first port in the load-sharing group is configured to be the “master” logical port. This is the reference port used in configuration commands. It can be thought of as the virtual port representing the entire port group.

Table 3-8 shows the allowable load-sharing port group combinations for the Switch 9000.

**Table 3-8** Port Combinations for the Switch 9000

Load-sharing Group	1	2	3	4	5	6	7	8
4-port groups				x	x	x	x	
2-port groups		x	x	x	x	x	x	

When you define a load-sharing group, you assign a group of ports to a single, logical port number. To enable or disable a load-sharing group, use the following commands:

```
enable sharing <master_port> grouping <portlist>
disable sharing <master_port>
```

The following example defines a load-sharing group that contains ports 4 through 7, and uses the first port in the group as the master logical port 4:

```
enable sharing 4 grouping 4-7
```

In this example, logical port 4 represents physical ports 4 through 7.



*When using load sharing, you should always reference the master logical port of the load-sharing group (port 4 in the previous example) when configuring or viewing VLANs. VLANs configured to use other ports in the load-sharing group will have those ports deleted from the VLAN when load sharing becomes enabled.*

### Verifying the Load Sharing Configuration

The `show port config` output screen indicates the ports that are involved in load sharing, and the master logical port identity.

### Current Limitations of Load Sharing

The following describes implementation restrictions that currently apply to load sharing:

- The load-sharing group must not participate in a spanning tree. If the VLANs using the load-sharing group are also members of a spanning tree, the ports associated with the load-sharing group must be disabled.
- A port involved in a load-sharing group must not be disabled.

# 4

## COMMANDS

This chapter contains a description of each command-line interface command for the Switch 9000. It also provides the following information related to Switch 9000 commands:

- Command syntax
- Line editing commands
- Command history substitution

If an asterisk (\*) appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For example:

```
*3C16990#
```



*In order for configuration changes to be retained through a Switch power cycle or reboot, you **must** issue a **SAVE** command after you have made the change. For more information on the SAVE command, refer to Chapter 10.*

---

### Understanding the Command Syntax

This section describes the steps to take when entering a command. Refer to the sections that follow for detailed information on using the command-line interface.

To use the command-line interface, follow these steps:

- 1 When entering a command at the prompt, ensure that you have the appropriate privilege level.

Most configuration commands require you to have the Administrator privilege level.

- 2 Enter the command name.

If the command does not include a parameter, skip to Step 3. If the command requires more information, or if you want to include optional parameters, continue to Step 2a.

- a If the command has additional parameters include them after the command name.
- b If the command includes a parameter, enter the parameter name, and its values.

The parameters values may include numerics, strings, or addresses, depending on the parameter.

- 3 After entering the complete command, press [Return].

### Syntax Helper

The command-line interface has a built-in syntax helper. If you are unsure of the complete syntax for a particular command, enter as much of the command as possible. The syntax helper will provide you with a list of options for the remainder of the command.

The syntax helper also provides assistance if you have entered an incorrect command.

### Command Completion

The Switch provides command completion by way of the [Tab] key. If you enter a partial command, pressing the [Tab] key fills in the remainder of the command. If command options exist, they are displayed. The full command is then redisplayed and the cursor is placed at the end of the command.

### Abbreviated Syntax

Abbreviated syntax is the shortest, unambiguous, allowable abbreviation of a command, parameter, or value. Typically, this is the first three letters of the command.

### Command Shortcuts

All named components of the Switch configuration must have a unique name. When you enter a command to configure a named component, you do not need to use the keyword of the component. For example, to create a VLAN, you must enter a unique VLAN name:

```
create vlan engineering
```

Once you have created the VLAN with a unique name, you can then eliminate the keyword *vlan* from all other commands that require the name to be entered. For example the following command:

```
config vlan engineering add port 1-3,6
```

could use the following shortcut:

```
config engineering add port 1-3, 6
```

### Numerical Ranges

Commands that require you to enter one or more port numbers use the parameter, `<portlist>`, in the syntax. A portlist can be a range of numbers, for example:

```
port 1-3
```

You can add additional port numbers to the list, separated by a comma:

```
port 1-3,6,8
```

### Names

All named components of the Switch configuration must have a unique name. Names must begin with an alphabetical character delimited by white space, unless enclosed in quotation marks.

### Symbols

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table 4-1 summarizes command syntax symbols.

**Table 4-1** Command Syntax Symbols

Symbol	Description
angle brackets < >	Enclose a variable or value. You must specify the variable or value. For example, in the syntax <pre>config vlan &lt;name&gt; ipaddress &lt;ip_address&gt;</pre> you must supply a VLAN name for <code>&lt;name&gt;</code> and an address for <code>&lt;ip_address&gt;</code> when entering the command. Do not type the angle brackets.
square brackets [ ]	Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax <pre>disable vlan [&lt;name&gt;   all]</pre> you must specify either the VLAN name for <code>&lt;name&gt;</code> , or the keyword "all" when entering the command. Do not type the square brackets.

(continued)

**Table 4-1** Command Syntax Symbols (continued)

Symbol	Description
vertical bar	<p>Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax</p> <pre>config snmp community [read   write] &lt;string&gt;</pre> <p>you must specify either the read or write community string in the command. Do not type the vertical bar.</p>
braces { }	<p>Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>show vlan {&lt;name&gt;   all}</pre> <p>you can specify either a particular VLAN or the keyword "all." If you do not specify an argument, the command will show all VLANs. Do not type the braces.</p>

## Line-Editing Commands

Table 4-2 describes the line-editing commands available using the command-line interface.

**Table 4-2** Line-Editing Commands

Command	Description
Backspace	Deletes character to the left of cursor and shifts remainder of line to left.
Delete or [Ctrl] + D	Deletes character under cursor and shifts remainder of line to left.
[Ctrl] + K	Deletes characters from under cursor to the end of the line.
Insert	Toggles on and off. When toggled on, inserts text and pushes previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [Ctrl]+A	Moves cursor to first character in line.
End or [Ctrl]+E	Moves cursor to last character in line.
[Ctrl]+L	Clears the screen and moves the cursor to the beginning of the line.
Up Arrow	Displays the previous command in the command history buffer, and places cursor at end of command.
Down Arrow	Displays the next command in the command history buffer, and places cursor at end of command.



## Command History Substitution

The Switch 9000 “remembers” the last 50 commands you enter. You can display a list of these commands by using the following command:

```
history
```

## Common Commands

Table 4-3 describes common commands used to manage the Switch. Commands specific to a particular feature are described in the other chapters of this guide.

**Table 4-3** Common Commands

Command	Description
<code>create account [admin   user] &lt;username&gt; {&lt;password&gt;}</code>	Allows you to create a user account. For more information on creating accounts, refer to Chapter 3.
<code>create vlan &lt;name&gt;</code>	Allows you to create a VLAN. For more information on VLANs, refer to Chapter 5.
<code>config account &lt;username&gt; {&lt;password&gt;}</code>	Allows you to configure a user account password.
<code>config time &lt;time&gt;</code>	Allows you to configure the system date and time. The format for <time> is: <i>mm/dd/yyyy hh:mm:ss</i> The time uses a 24 hour clock format.
<code>config vlan &lt;name&gt; ipaddress &lt;ip_address&gt; {&lt;mask&gt;}</code>	Allows you to configure an IP address and subnet mask for a VLAN.
<code>enable bootp vlan [&lt;name&gt;   all]</code>	Allows you to enable BOOTP for one or more VLANs. For more information on using BOOTP, refer to Chapter 3.
<code>clear session &lt;number&gt;</code>	Allows you to terminate a Telnet session from the Switch.
<code>disable bootp vlan [&lt;name&gt;   all]</code>	Allows you to disable BOOTP for one or more VLANs.
<code>disable port &lt;portlist&gt;</code>	Allows you to disable or partition a port.
<code>disable telnet</code>	Allows you to disable Telnet access to the Switch.
<code>delete account &lt;username&gt;</code>	Allows you to delete a user account.
<code>delete vlan &lt;name&gt;</code>	Allows you to delete a VLAN.
<code>logout   quit</code>	Allows you to logout of a console or Telnet session. If used during a Telnet session, also closes the TCP Telnet session.

(continued)

**Table 4-3** Common Commands (continued)

Command	Description
<code>unconfig switch {all}</code>	Allows you to reset all Switch parameters (with the exception of defined VLANs and IP addresses) to the factory defaults. If you specify the keyword "all", the IP addresses are reset as well.

## Switch 9000 Commands

The tables in this section list all of the commands used on the Switch 9000. The commands are organized by the following categories:

- General Switch commands
- User account commands
- Switch management commands
- VLAN commands
- Protocol commands
- FDB commands
- Port commands
- PACE commands
- STP commands
- Basic IP commands
- *IP Address Resolution Protocol (ARP)* commands
- IP route table commands
- ICMP commands
- RIP commands
- Logging commands
- Configuration and image commands

## General Switch Commands

Table 4-4 describes general Switch commands.

**Table 4-4** General Switch Commands

Command	Description
<code>show switch</code>	<p>Displays the current Switch information, including:</p> <ul style="list-style-type: none"> <li>■ sysName, sysLocation, sysContact</li> <li>■ MAC address</li> <li>■ current date and time, and system uptime</li> <li>■ operating environment (temperature, fans, and power supply status)</li> <li>■ NVRAM image information (primary/secondary image, date, time, size, version)</li> <li>■ NVRAM configuration information (primary/secondary configuration, date, time, size, version)</li> <li>■ Scheduled reboot information</li> <li>■ System serial number and reworks indicator</li> <li>■ Software platform</li> <li>■ System ID</li> <li>■ Power supply and fan status</li> </ul>
<code>show version</code>	<p>Displays the hardware and software versions currently running on the Switch. Also displays the Switch serial number.</p>
<code>show memory</code>	<p>Displays summary system configuration and memory utilization statistics for the CPU system DRAM.</p>
<code>reboot</code>	<p>Allows you to reboot the Switch. The Switch will ask for confirmation and then reboot.</p>
<code>config time &lt;time&gt;</code>	<p>Allows you to configure the system date and time. The format for &lt;time&gt; is:</p> <p>mm/dd/yyyy hh:mm</p> <p>The time uses a 24-hour clock format.</p>
(continued)	

**Table 4-4** General Switch Commands (continued)

Command	Description
<code>config devicemode [bridging   iprouting]</code>	<p>Allows you to configure the operating mode of the Switch. Specify:</p> <ul style="list-style-type: none"> <li>■ <code>bridging</code> — Layer 2 bridging functions only</li> <li>■ <code>iprouting</code> — Bridging and IP unicast routing functions</li> </ul> <p>If this command is used to change the operating mode of the Switch 9000 once it is up and running, it causes the Switch to save the configuration and reboot. The default operating mode is “iprouting.”</p>
<code>unconfig switch {all}</code>	<p>Allows you to reset all Switch parameters (with the exception of defined VLANs and IP addresses) to the factory defaults. If you specify the keyword “all”, the IP addresses are reset as well.</p>
<code>ping {continuous} {size &lt;number&gt;} &lt;ipaddress&gt;</code>	<p>Allows you to send ICMP echo messages to a remote IP device. Specify:</p> <ul style="list-style-type: none"> <li>■ <code>continuous</code> — ICMP echo messages should be sent continuously.</li> <li>■ <code>size &lt;n&gt;</code> — The size of the packet.</li> </ul>
<code>traceroute &lt;ipaddress&gt;</code>	<p>Allows you to trace the routed path between the Switch and a destination endstation.</p>
<code>clear counters</code>	<p>Allows you to clear all statistical counters for the Switch and ports.</p>

### User Account Commands

Table 4-5 describes user account commands

**Table 4-5** User Account Commands

Command	Description
<code>show account</code>	<p>Displays the account names, access level, number of successful and failed logon attempts, and the number of active sessions in the user database. This command is available only to admin level users.</p>
<code>create account [admin   user] &lt;username&gt; {&lt;password&gt;}</code>	<p>Allows you to create a user account.</p>
<code>delete account &lt;username&gt;</code>	<p>Allows you to delete a user account</p>
<code>config account &lt;username&gt; {&lt;password&gt;}</code>	<p>Allows you to change the password of an existing account.</p>

## Switch Management Commands

Table 4-6 describes Switch management commands

**Table 4-6** Switch Management Commands

Command	Description
<code>show management</code>	Displays network management configuration and statics including enable/disable states for Telnet and SNMP, SNMP community strings, authorized SNMP station list, SNMP trap receiver list, and logon statistics.
<code>show session</code>	Displays the currently active Telnet and console sessions communicating with the Switch. Provides the user name, IP address of the incoming Telnet session, whether a console session is currently active, and logon time. Sessions are numbered.
<code>clear session &lt;number&gt;</code>	Allows you to terminate a Telnet session from the Switch.
<code>logout   quit</code>	Allows you to logout of a console or Telnet session. If used during a Telnet session, also closes the TCP Telnet session.
<code>enable telnet</code>	Allows you to enable Telnet access to the Switch.
<code>disable telnet</code>	Allows you to disable Telnet access to the Switch.
<code>enable snmp access</code>	Allows you to turn on SNMP support for the Switch.
<code>disable snmp access</code>	Allows you to disable SNMP on the Switch.
<code>enable snmp trap</code>	Allows you to turn on SNMP trap support.
<code>disable snmp trap</code>	Allows you to prevent SNMP traps from being sent from the Switch.
<code>config snmp add &lt;ipaddress&gt;</code>	Allows you to add the IP address of an SNMP management station to the access list. Up to six address can be specified.
<code>config snmp delete [&lt;ipaddress&gt;   all]</code>	Allows you to delete the IP address of a specified SNMP management station or all SNMP management stations.
<code>config snmp add trapreceiver &lt;ipaddress&gt; {&lt;comm_string&gt;}</code>	Allows you to add the IP address of a specified trap receiver. A maximum of six trap receivers is allowed.
<code>config snmp delete trapreceiver [&lt;ipaddress&gt;   all]</code>	Allows you to delete the IP address of a specified trap receiver or all authorized trap receivers. If you delete all trap receiver addresses, any machine can have SNMP management access to the Switch.
<code>config snmp community [read   readwrite] &lt;string&gt;</code>	Allows you to configure the SNMP read and write community strings. The community string can have a maximum of 32 characters.

(continued)

**Table 4-6** Switch Management Commands (continued)

Command	Description
<code>config snmp syscontact &lt;string&gt;</code>	Allows you to configure the name of the system contact. A maximum of 32 characters is allowed
<code>config snmp sysname &lt;string&gt;</code>	Allows you to configure the name of the Switch. The sysname appears in the command line interface prompt. A maximum of 32 characters is allowed. The default sysname is 3C16990.
<code>config snmp syslocation &lt;string&gt;</code>	Allows you to configure the location of the Switch. A maximum of 32 characters is allowed.
<code>unconfig management</code>	Restores default values to all SNMP-related entries.

**VLAN Commands** Table 4-7 describes VLAN commands.

**Table 4-7** VLAN Commands

Command	Description
<code>show vlan {&lt;name&gt;   all}</code>	When used with the keyword "all", or with no named VLANs, displays a summary list of VLAN names with a portlist and associated status of each. When used with a named identifier, displays port information including membership list, IP address, tag information.
<code>create vlan &lt;name&gt;</code>	Allows you to create a named VLAN.
<code>delete vlan &lt;name&gt;</code>	Allows you to remove a VLAN.
<code>config vlan &lt;name&gt; [add   delete] &lt;portlist&gt; {tagged   untagged}</code>	Allows you to add and delete ports. You can specify tagged and untagged port(s). By default, ports are untagged.
<code>config vlan &lt;name&gt; tag &lt;vlanid&gt;</code>	Allows you to assign a numerical VLANid. The valid range is from 1 to 4095.
<code>config vlan &lt;name&gt; protocol [&lt;protocol_name&gt;   any]</code>	Allows you to configure a protocol based VLAN. If the keyword "any" is specified, then it becomes the default VLAN. All packets that cannot be classified into other protocol-based VLANs are assigned to the default VLAN of that port.
<code>config vlan &lt;name&gt; ipaddress &lt;ipaddress&gt; {&lt;mask&gt;}</code>	Allows you to assign an IP address and an optional mask to the VLAN.
<code>config dot1q ethertype &lt;ethertype&gt;</code>	Allows you to configure an IEEE 802.1Q Ethertype. Use this command if you have another switch that supports 802.1Q, but uses a different Ethertype. The default value used by the Switch is <b>8100</b> .
<code>unconfig vlan &lt;name&gt; ipaddress</code>	Allows you to remove the IP address associated with a VLAN.

**Protocol Commands** Table 4-8 describes protocol commands.

**Table 4-8** Protocol Commands

Command	Description
<code>show protocol {&lt;protocol_name&gt;   all}</code>	Allows you to display protocol-related information, including: <ul style="list-style-type: none"> <li>■ Protocol name</li> <li>■ List of protocol fields</li> <li>■ List of VLANs that use this protocol</li> </ul>
<code>create protocol &lt;protocol_name&gt;</code>	Allows you to create a user-defined protocol.
<code>delete protocol &lt;protocol_name&gt;</code>	Allows you to remove a protocol.
<code>config protocol &lt;protocol_name&gt; add &lt;protocol_type&gt; &lt;hex_value&gt;</code>	Allows you to configure a protocol filter. Supported protocol types include: <ul style="list-style-type: none"> <li>■ EtherType</li> <li>■ LLC</li> <li>■ SNAP</li> </ul>

**FDB Commands** Table 4-9 describes FDB commands.

**Table 4-9** FDB Commands

Command	Description
<code>show fdb {all   &lt;mac_address&gt;   vlan &lt;name&gt;   &lt;portlist&gt;   permanent}</code>	Displays the forwarding database contents including MAC address, associated VLAN, port, age of entry configuration method, and status. Providing one of the options acts as a filter on the display. Providing a VLAN name displays all entries for the VLAN. Use the MAC address to locate a specific entry in the FDB.
<code>clear fdb {all   &lt;mac_address&gt;   vlan &lt;name&gt;   &lt;portlist&gt; }</code>	Allows you to clear dynamic FDB entries that match the filter. Use the keyword "all" to clear all dynamic entries.

(continued)

**Table 4-9** FDB Commands (continued)

Command	Description
<code>create fdbentry &lt;mac_address&gt; vlan &lt;name&gt; &lt;portlist&gt;</code>	<p>Allows you to create a permanent FDB entry. Specify the following:</p> <ul style="list-style-type: none"> <li>■ <code>mac_address</code> — device MAC address, using colon separated bytes</li> <li>■ <code>name</code> — VLAN associated with MAC address</li> <li>■ <code>portlist</code> — port number associated with MAC address</li> </ul> <p>If more than one port number is associated with a permanent MAC entry, packets will be multicast to the multiple destinations.</p>
<code>delete fdbentry &lt;mac_address&gt; vlan &lt;name&gt;</code>	Allows you to delete a permanent FDB entry.
<code>config fdb agingtime &lt;number&gt;</code>	Allows you to configure the FDB ageing time. The range is 15 through 1,000,000 seconds. The default value is 1800 seconds. A value of 0 indicates that the entry should never be aged out.

**Port Commands**      Table 4-10 describes port commands.

**Table 4-10** Port Commands

Command	Description
<code>show port &lt;portlist&gt; config</code>	Displays state, link status, speed, and autonegotiation setting for each port.
<code>show port &lt;portlist&gt; stats</code>	Displays port information including physical layer configuration and statistics.
<code>show port &lt;portlist&gt; errors</code>	Displays error information for one or more ports.
<code>show port &lt;portlist&gt; collisions</code>	Displays real-time collision statistics.
<code>show port &lt;portlist&gt; packet</code>	Displays a histogram of packet statistics for one or more ports.
<code>show port &lt;portlist&gt; util</code>	Displays port utilization by percentage, bytes per second, or packets per second. Use the space bar to toggle between percentage, bytes per second, or packets per second. Use the clear counters command to reset values.
<code>config port &lt;portlist&gt; auto on</code>	Allows you to toggle 802.3z link startup autonegotiation on.
<code>config port &lt;portlist&gt; auto off</code>	Allows you to toggle 802.3z link startup autonegotiation off.

(continued)



**Table 4-10** Port Commands

Command	Description
<code>enable port &lt;portlist&gt;</code>	Allows you to enable one or more ports.
<code>disable port &lt;portlist&gt;</code>	Allows you to disable one or more ports.

**PACE Commands** Table 4-11 describes PACE commands.

**Table 4-11** PACE Commands

Command	Description
<code>enable pace</code>	Allows you to enable recognition of the PACE bit.
<code>disable pace</code>	Allows you to disable recognition of the PACE bit.

**STP Commands** Table 4-12 describes STP commands.

**Table 4-12** STP Commands

Command	Description
<code>show stpd {&lt;stpd_name&gt;   all}</code>	Displays STP information for one or all STPDs on the Switch.
<code>show stpd &lt;stpd_name&gt; port &lt;portlist&gt;</code>	Displays port-specific STP information, including the forwarding state of each port.
<code>create stpd &lt;stpd_name&gt;</code>	Allows you to create an STPD. When created, an STPD has the following default parameters: <ul style="list-style-type: none"> <li>■ Bridge priority — 32,768</li> <li>■ Hello time — 2 seconds</li> <li>■ Forward delay — 15 seconds</li> </ul>
<code>delete stpd &lt;stpd_name&gt;</code>	Allows you to remove an STPD. An STPD can only be removed if all VLANs have been deleted from it.
<code>config stpd &lt;stpd_name&gt; add vlan &lt;name&gt;</code>	Allows you to add a VLAN to the STPD.
<code>config stpd &lt;stpd_name&gt; delete vlan [&lt;name&gt;   all]</code>	Allows you to remove one or all VLANs from an STPD. If <code>all</code> is specified, the association between the STPD and VLAN is removed, but both still exist.
<code>config stpd &lt;stpd_name&gt; hellotime &lt;value&gt;</code>	Allows you to specify the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge.  The range is 1 through 10. The default setting is 2 seconds.

(continued)

**Table 4-12** STP Commands (continued)

Command	Description
<code>config stpd &lt;stpd_name&gt; forwarddelay &lt;value&gt;</code>	Allows you to specify the time (in seconds) that the ports on this STPD spend in the listening and learning states when the Switch is the Root Bridge.  The range is 4 through 30. The default setting is 15 seconds.
<code>config stpd &lt;stpd_name&gt; maxage &lt;value&gt;</code>	Allows you to specify the maximum age of a BPDU in this STPD.  The range is 6 through 40. The default setting is 20 seconds.  Note that the time must be greater than, or equal to 2 x (Hello Time + 1) and less than, or equal to 2 x (Forward Delay -1).
<code>config stpd &lt;stpd_name&gt; priority &lt;value&gt;</code>	Allows you to specify the priority of the STPD. By changing the priority of the Switch, you can make it more or less likely to become the Root Bridge.  The range is 0-65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.
<code>config stpd &lt;stpd_name&gt; port cost &lt;value&gt; &lt;portlist&gt;</code>	Allows you to specify the path cost of the port in this STPD.  The range is 1-65,535. The Switch automatically assigns a default path cost of 1.
<code>config stpd &lt;stpd_name&gt; port priority &lt;value&gt; &lt;portlist&gt;</code>	Allows you to specify the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the Root Port.  The range is 0-255. The default setting is 128. A setting of 0 indicates the lowest priority.
<code>enable stpd [&lt;stpd_name&gt;   all]</code>	Allows you to enable STP for one or more STPDs. The default setting is disabled.
<code>disable stpd [&lt;stpd_name&gt;   all]</code>	Allows you to disable the STP mechanism on a particular STPD, or for all STPDs.
<code>enable stpd port &lt;portlist&gt;</code>	Allows you to enable STP on one or more ports.
<code>disable stpd port &lt;portlist&gt;</code>	Allows you to disable STP on one or more ports. Disabling STP on one or more ports puts those ports in FORWARDING state; all BPDUs received on those ports will be disregarded.
<code>unconfig stpd {&lt;stpd_name&gt;   all}</code>	Allows you to restore default STP values to a particular STPD or to all STPDs.

## Basic IP Commands

Table 4-13 describes basic IP commands.

**Table 4-13** Basic IP Commands

Command	Description
<code>show ipconfig {vlan [&lt;name&gt;   all]}</code>	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none"> <li>■ IP address, subnet mask</li> <li>■ IP forwarding information</li> <li>■ BOOTP configuration</li> <li>■ VLAN name, VLANid</li> </ul>
<code>show ipstats {vlan [&lt;name&gt;   all]}</code>	Displays statistics of packets handled by the CPU, including the following: <ul style="list-style-type: none"> <li>■ inpackets, outpackets</li> <li>■ ICMP/IGMP statistics</li> <li>■ IRDP statistics</li> </ul>
<code>show ipfdb {&lt;ipaddress&gt; &lt;netmask&gt;   vlan &lt;name&gt;   all}</code>	Displays the contents of the IP forwarding database table. Use for technical support purposes.
<code>clear ipfdb [&lt;ipaddress&gt; &lt;netmask&gt;   vlan &lt;name&gt;   all]</code>	Allows you to clear the dynamic entries in the IP forwarding database table.
<code>enable ipforwarding {vlan &lt;name&gt;   all}</code>	Allows you to enable IP forwarding to an IP interface. If "all" is specified, then all the configured IP interfaces are affected. If no optional argument is provided, the "all" is assumed. Other IP configuration is not affected. When new IP interfaces are added, the interface is configured to have ipforwarding disabled by default.
<code>disable ipforwarding {vlan &lt;name&gt;   all}</code>	Allows you to disable IP forwarding on one or all IP interfaces.
<code>enable ipforwarding broadcast {vlan &lt;name&gt;   all}</code>	Allows you to enable forwarding of IP broadcast traffic on an IP interface. If "all" is specified, then all the configured IP interfaces are affected. If no optional argument is provided, then "all" is assumed. Other IP configuration is not affected. When new IP interfaces are added, the default is to have broadcast enabled.
<code>disable ipforwarding broadcast {vlan &lt;name&gt;   all}</code>	Allows you to disable IP broadcast forwarding on one or all IP interfaces.
<code>enable bootp vlan [&lt;name&gt;   all]</code>	Allows you to enable the generation and processing of BOOTP packets on a VLAN. The default setting is enabled for all VLANs.

(continued)

**Table 4-13** Basic IP Commands (continued)

Command	Description
<code>disable bootp vlan [&lt;name&gt;   all]</code>	Allows you to disable the generation and processing of BOOTP packets.
<code>enable bootprelay</code>	Allows you to enable the BOOTP relay function on the router.
<code>disable bootprelay</code>	Allows you to disable the BOOTP relay function on the router.
<code>config bootprelay add &lt;ipaddress&gt;</code>	Allows you to add IP addresses to be used as IP destinations to forward BOOTP packets.
<code>config bootprelay delete [&lt;ipaddress&gt;   all]</code>	Allows you to delete one or all IP addresses that were used as IP destinations to forward BOOTP packets.

**IP ARP Commands** Table 4-14 describes IP ARP commands.

**Table 4-14** IP ARP Commands

Command	Description
<code>show iparp {&lt;ipaddress&gt;   vlan &lt;name&gt;   all   permanent}</code>	Displays the current Address Resolution Protocol (ARP) cache for a selected IP address, VLAN, or all entries. With no options, information for all VLANs is displayed. Information displayed includes IP address, MAC address, aging timer value, VLAN name, VLANid, and port number.
<code>clear iparp [&lt;ipaddress&gt;   vlan &lt;name&gt;   all]</code>	Allows you to remove dynamic entries in the IP ARP table.
<code>config iparp add &lt;ipaddress&gt; &lt;mac_address&gt;</code>	Allows you to add a permanent IP ARP entry to the system. The IP address is used to match the IP interface address to locate a suitable interface.
<code>config iparp delete &lt;ipaddress&gt;</code>	Allows you to delete an IP ARP entry from the table.

## IP Route Table Commands

Table 4-15 describes IP route table commands.

**Table 4-15** IP Route Table Commands

Command	Description
<code>show iproute {vlan {&lt;name&gt;   all   permanent   &lt;ipaddress&gt; &lt;netmask&gt;}</code>	Allows you to display the contents of the IP routing table.
<code>config iproute add default &lt;gateway&gt; {&lt;metric&gt;}</code>	Allows you to add a default gateway to the routing table. A default gateway must be located on a configured IP interface. If no metric is specified, the default metric of 1 is used.
<code>config iproute delete default &lt;gateway&gt;</code>	Allows you to delete a default gateway.
<code>config iproute add &lt;ipaddress&gt; &lt;mask&gt; &lt;gateway&gt; {&lt;metric&gt;}</code>	Allows you to add a static address to the routing table. Use a value of 255.255.255.255 for <code>mask</code> to indicate a host entry.
<code>config iproute delete &lt;ipaddress&gt; &lt;mask&gt; &lt;gateway&gt;</code>	Allows you to delete a static address from the routing table.
<code>config iproute add blackhole &lt;ipaddress&gt; &lt;mask&gt;</code>	Allows you to add a blackhole address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.
<code>config iproute delete blackhole &lt;ipaddress&gt; &lt;mask&gt;</code>	Allows you to delete a blackhole address from the routing table.

## ICMP Commands

Table 4-16 describes the commands used to configure the ICMP protocol.

**Table 4-16** ICMP Commands

Command	Description
<code>enable icmp redirects {vlan &lt;name&gt;   all}</code>	Allows you to enable generation of ICMP redirect messages on one or more VLANs. The default setting is enabled.
<code>disable icmp redirects {vlan &lt;name&gt;   all}</code>	Allows you to disable the generation of ICMP redirects on one or more VLANs.
<code>enable icmp unreachable {vlan &lt;name&gt;   all}</code>	Allows you to enable the generation of ICMP unreachable messages on one or more VLANs. The default setting is enabled.
<code>disable icmp unreachable</code>	Allows you to disable the generation of ICMP unreachable messages on one or more VLANs.

(continued)

**Table 4-16** ICMP Commands (continued)

Command	Description
<code>enable icmp userredirects</code>	Allows you to enable the modification of route table information when an ICMP redirect message is received. The default setting is disabled.
<code>disable icmp userredirects</code>	Allows you to disable the changing of routing table information when an ICMP redirect message is received.
<code>enable irdp {vlan &lt;name&gt;   all}</code>	Allows you to enable the generation of ICMP router advertisement messages on one or more VLANs. The default setting is enabled.
<code>disable irdp {vlan &lt;name&gt;   all}</code>	Allows you to disable the generation of router advertisement messages on one or more VLANs.
<code>config irdp [multicast   broadcast]</code>	Allows you to configure the destination address of the router advertisement messages. The default setting is broadcast.
<code>config irdp &lt;mininterval&gt; &lt;maxinterval&gt; &lt;lifetime&gt; &lt;preference&gt;</code>	Allows you to configure the router advertisement message timers, using seconds. Specify: <ul style="list-style-type: none"> <li>■ <code>mininterval</code> — The minimum amount of time between router advertisements. The default setting is 450 seconds.</li> <li>■ <code>maxinterval</code> — The maximum time between router advertisements. The default setting is 600 seconds.</li> <li>■ <code>lifetime</code> — The default setting is 1,800 seconds.</li> <li>■ <code>preference</code> — The preference level of the router. An IRDP client always uses the router with the highest preference level. Change this setting to encourage or discourage the use of this router. The default setting is 0.</li> </ul>
<code>unconfig icmp</code>	Allows you to reset all ICMP settings to the default values.
<code>unconfig irdp</code>	Allows you to reset all router advertisement settings to the default values.
<code>disable irdp {vlan &lt;name&gt;   all}</code>	Allows you to disable the generation of router advertisement messages on one or more VLANs.

**RIP Commands** Table 4-17 describes the commands used to configure the RIP protocol.

**Table 4-17** RIP Commands

Command	Description
<code>show rip {vlan &lt;name&gt;   all}</code>	Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following: <ul style="list-style-type: none"> <li>■ Packets transmitted</li> <li>■ Packets received</li> <li>■ Bad packets received</li> <li>■ Bad routes received</li> <li>■ Number of RIP peers</li> <li>■ Peer information</li> </ul>
<code>enable rip</code>	Allows you to enable <b>RIP</b> .
<code>disable rip</code>	Allows you to disable <b>RIP</b> .
<code>config rip add {vlan &lt;name&gt;   all}</code>	Allows you to configure RIP on an IP interface. If no VLAN is specified, then "all" is assumed. When an IP interface is created, per interface RIP configuration is enabled by default.
<code>config rip delete {vlan &lt;name&gt;   all}</code>	Allows you to disable RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
<code>enable rip aggregation</code>	Allows you to enable RIP aggregation of subnet information on a RIP version 2 interface. The default setting is enabled.
<code>disable rip aggregation</code>	Allows you to disable the RIP aggregation of subnet information on a RIP version 2 interface.
<code>enable rip splithorizon</code>	Allows you to enable the split horizon algorithm for RIP. Default setting is enabled.
<code>disable rip splithorizon</code>	Allows you to disable split horizon.
<code>enable rip poisonreverse</code>	Allows you to enable the split horizon with poison-reverse algorithm for RIP. The default setting is enabled.
<code>disable rip poisonreverse</code>	Allows you to disable poison reverse.
<code>enable rip triggerupdate</code>	Allows you to enable triggered updates. <i>Triggered updates</i> are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
<code>disable rip triggerupdate</code>	Allows you to disable triggered updates.

(continued)

**Table 4-17** RIP Commands (continued)

Command	Description
<code>enable rip exportstatic</code>	Allows you to enable the advertisement of static routes using RIP. The default setting is enabled.
<code>disable rip exportstatic</code>	Allows you to disable the filtering of static routes.
<code>config rip updatetime {&lt;delay&gt;}</code>	Allows you to change the periodic RIP update timer. The default setting is 30 seconds.
<code>config rip routetimeout {&lt;delay&gt;}</code>	Allows you to configure the route timeout. The default setting is 180 seconds.
<code>config rip garbagetime {&lt;delay&gt;}</code>	Allows you to configure the RIP garbage time. The default setting is 120 seconds.
<code>config rip txmode [none   v1only   v1comp   v2only] {vlan &lt;name&gt;   all}</code>	<p>Allows you to change the RIP transmission mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> <li>■ none — Do not transmit any packets on this interface.</li> <li>■ v1only — Transmit RIP version 1 format packets to the broadcast address.</li> <li>■ v1comp — Transmit version 2 format packets to the broadcast address.</li> <li>■ v2only — Transmit version 2 format packets to the RIP multicast address.</li> </ul> <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is "v2only".</p>
<code>config rip rxmode [none   v1only   v2only   any] {vlan &lt;name&gt;   all}</code>	<p>Allows you to change the RIP receive mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> <li>■ none — Drop all received RIP packets.</li> <li>■ v1only — Accept only RIP version 1 format packets.</li> <li>■ v2only — Accept only RIP version 2 format packets.</li> <li>■ any — Accept both version 1 and version 2 packets.</li> </ul> <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is "any".</p>
<code>unconfig rip {vlan &lt;name&gt;   all}</code>	Allows you to reset all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.



## Logging Commands

Table 4-18 describes Switch logging commands.

**Table 4-18** Logging Commands

Command	Description
<code>show log config</code>	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
<code>show log {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	<p>Displays the current snapshot of the log. Options include:</p> <ul style="list-style-type: none"> <li>■ <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.</li> </ul>
<code>clear log</code>	Allows you to clear the log.
<code>config log display {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	<p>Allows you to configure the real-time log display. Options include:</p> <ul style="list-style-type: none"> <li>■ <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.</li> </ul>

(continued)

**Table 4-18** Logging Commands (continued)

Command	Description
<code>config syslog &lt;ipaddress&gt; &lt;facility&gt; {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	Allows you to configure the syslog host address and filter messages sent to the syslog host. Options include: <ul style="list-style-type: none"><li>■ <code>ipaddress</code> — The IP address of the syslog host.</li><li>■ <code>facility</code> — The syslog facility level for local use.</li><li>■ <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, only critical priority messages are sent to the syslog host.</li><li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are sent to the syslog host.</li></ul>
<code>enable log display</code>	Allows you to enable the log display.
<code>enable syslog</code>	Allows you to enable logging to a remote syslog host.
<code>disable log display</code>	Allows you to disable the log display.
<code>disable syslog</code>	Allows you to disable logging to a remote syslog host.

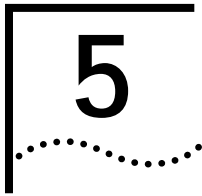
## Configuration and Image Commands

Table 4-19 describes configuration and image commands

**Table 4-19** Configuration and Image Commands

Command	Description
<code>save {config} {primary   secondary}</code>	Allows you to save the current configuration of the Switch to NVRAM. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the configuration area currently in use.
<code>use config {primary   secondary}</code>	Allows you to configure the Switch to use a particular configuration on the next reboot. Options include the primary configuration area, the secondary configuration area, or an imported ASCII file. If not specified, the Switch will use the primary configuration area.
<code>use image {primary   secondary}</code>	Allows you to configure the Switch to use a particular image on the next reboot. If not specified, the Switch will use the primary image.
<code>download image &lt;ipaddress&gt; &lt;filename&gt; {primary   secondary}</code>	Allows you to download a new image from a TFTP server. You must specify the IP address of the TFTP server and the image filename. You can optionally specify if you want the file downloaded to the primary or secondary image. If you do not specify, the file is downloaded to the primary image.





# VIRTUAL LANs (VLANs)

Setting up *Virtual Local Area Networks (VLANs)* on the Switch 9000 eases many time-consuming tasks of network administration while increasing efficiency in network operations.

This chapter describes the VLAN concepts and explains how to implement VLANs on the Switch 9000.

---

## Overview of Virtual LANs

A VLAN is a group of location- and topology-independent devices, for example a group of users (workstations) and the server to which they connect, that communicate as if they are on the same physical LAN. This means that LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups that you create with the command-line interface.

**Benefits** Implementing VLANs on your networks has the following advantages:

- **It eases the change and movement of devices.**

With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each endstation must be updated manually.

For example, with a VLAN, if an endstation in VLAN *Marketing* is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is in VLAN *Marketing*.

- **It helps to control traffic.**

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether they require it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

- **It provides extra security.**

Devices within each VLAN can only communicate with member devices in the same VLAN. If a device in VLAN *Marketing* must communicate with devices in VLAN *Sales*, the traffic must cross a routing device.

**Types of VLANs** Switch 9000 VLANs can be created according to the following criteria:

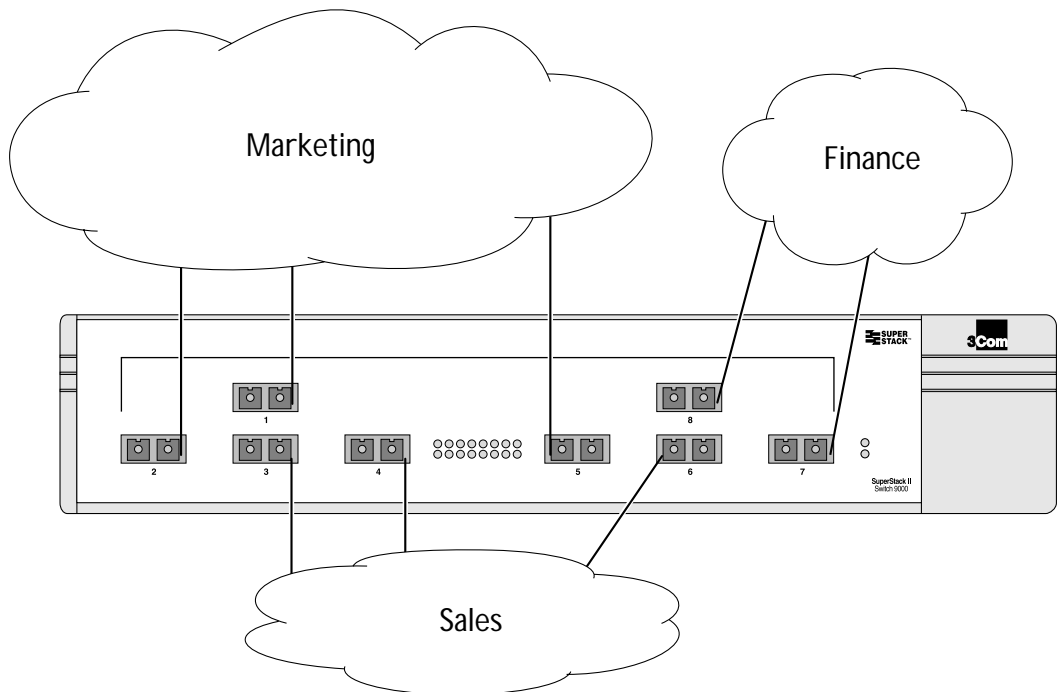
- Physical port
- IEEE 802.1Q tag
- Ethernet protocol type
- A combination of these criteria

#### **Port-Based VLANs**

In a port-based VLAN, a VLAN name is given to a group of one or more ports on the Switch. A Switch port can be a member of only one port-based VLAN.

For example, in Figure 5-1, the VLANs are configured as followings:

- Ports 1, 2, and 5 are part of VLAN *Marketing*
- Ports 3, 4, and 6 are part of VLAN *Sales*
- Ports 7 and 8 are part of VLAN *Finance*



**Figure 5-1** Example of a port-based VLAN

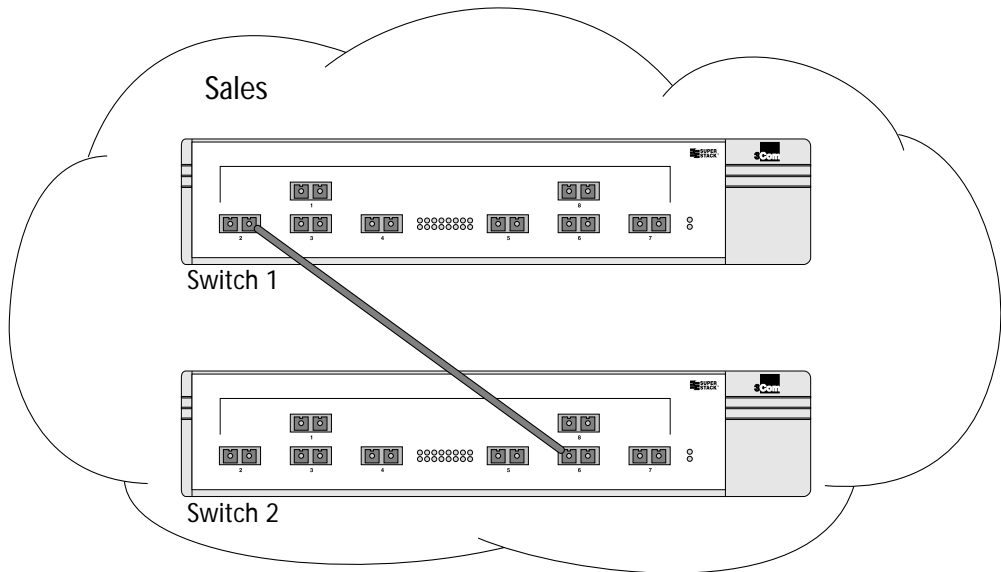
Even though they are physically connected to the same Switch, in order for the members of the different VLANs to communicate, the traffic must go through the IP routing functionality provided in the Switch 9000. This means that each VLAN must be configured as a router interface with a unique IP address.

## Expanding Port-Based VLANs Across Switches

To create a port-based VLAN that spans two Switches you must do two things:

- Assign the port on each Switch to the VLAN.
- Cable the two Switches together using one port on each Switch per VLAN.

Figure 5-2 illustrates a single VLAN that spans two Switches. All ports on both Switches belong to VLAN *Sales*. The two Switches are connected using port 2 on Switch 1, and port 6 on Switch 2.

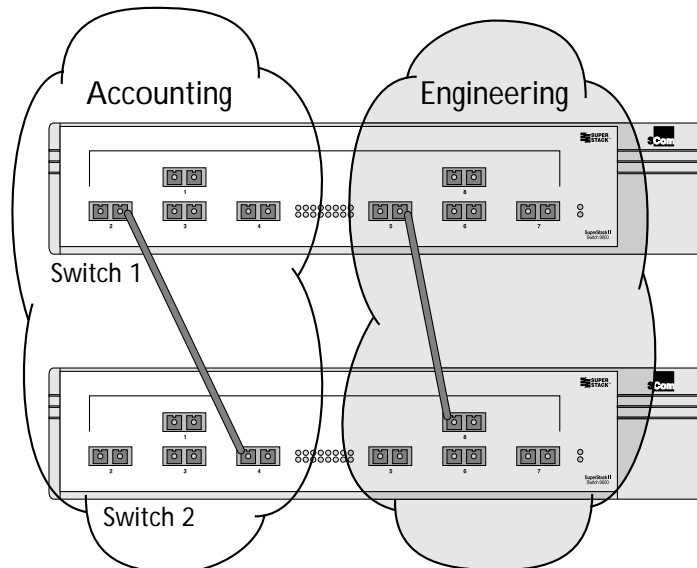


**Figure 5-2** Single port-based VLAN spanning two Switches

In a port-based VLAN, to create multiple VLANs that span two Switches, a port on Switch 1 must be cabled to a port on Switch 2 for each VLAN that you want to create. At least one port on each Switch must be a member of one of the VLANs, as well.



Figure 5-3 illustrates two VLANs spanning two Switches. On Switch 1, ports 1–4 are part of VLAN *Accounting*; ports 5–8 are part of VLAN *Engineering*. On Switch 2, ports 1–4 are part of VLAN *Accounting*; ports 5–8 are part of VLAN *Engineering*. VLAN *Accounting* spans Switch 1 and Switch 2 by way of a connection between Switch 1 port 2 and Switch 2 port 4. VLAN *Engineering* spans Switch 1 and Switch 2 by way of a connection between Switch 1 port 5 and Switch 2 port 8.



**Figure 5-3** Two port-based VLANs spanning two Switches

Using these steps, you can create multiple VLANs that span multiple Switches, in a daisy-chained fashion. Each Switch must have a dedicated port for each VLAN. Each dedicated port must be connected to a port that is a member of its VLAN on the next Switch.



*To avoid the creation of a bridging loop, you must configure the VLANs prior to cabling the ports.*

## Tagged VLANs

The Switch 9000 uses the IEEE 802.1Q D4 draft standard for rules associated with VLAN tagging.

*Tagging* is a process that inserts a marker (called a *tag*) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the *VLANid*.

## Uses of Tagged VLANs

Tagging is most commonly used to create VLANs that span Switches. The Switch-to-Switch connections are called *trunks*. Using tags, multiple VLANs can span multiple Switches using one or more trunks. In a port-based VLAN, each VLAN requires its own pair of trunk ports, as shown in Figure 5-3. Using tags, multiple VLANs can span two Switches with a single trunk.

Another benefit of tagged VLANs is the ability to have a port be a member of multiple VLANs. This is particularly useful if you have a device (such as a server) that must belong to multiple VLANs. The device must have a NIC that supports 802.1Q tagging.

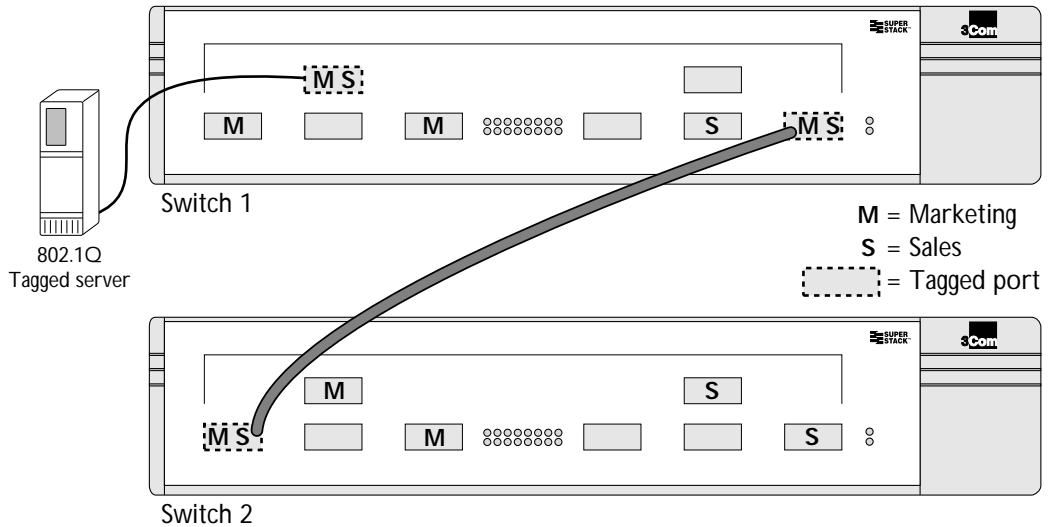
A single port can be a member of only one port-based VLAN. All additional VLAN membership for the port must be done using tags. In addition to configuring the VLAN tag for the port, the server must have a *Network Interface Card (NIC)* that supports 802.1Q tagging.

## Assigning a VLAN Tag

When a tag-based VLAN is created, it is given a name and a unique tag (VLANid). Ports are then assigned to the VLAN. As you assign each port, you can decide if the port will use the tag.

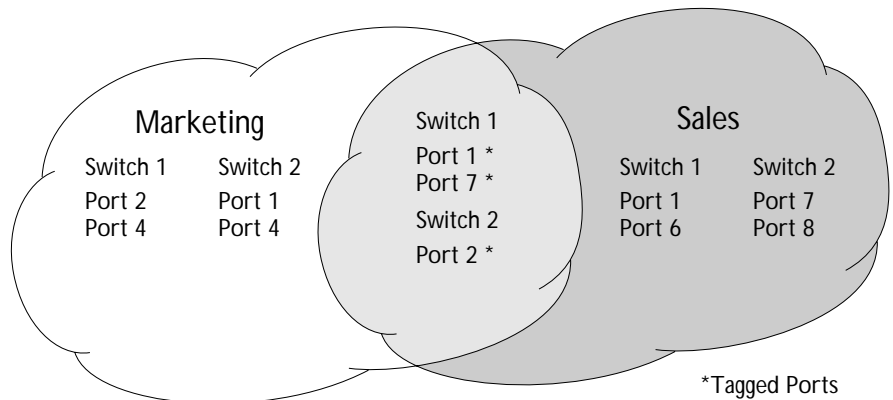
Not all ports in the VLAN must be tagged. As traffic from a port is forwarded out of the Switch, the Switch determines (in real time) if each destination port should use tagged or untagged packet formats for that VLAN. The Switch adds and strips tags, as required, by the port configuration.

Figure 5-4 illustrates the physical view of a network that uses tagged and untagged traffic.



**Figure 5-4** Physical diagram of tagged and untagged traffic

Figure 5-5 shows a logical diagram of the same network.



**Figure 5-5** Logical view of tagged and untagged traffic

In Figure 5-4 and Figure 5-5:

- The trunk port on each Switch carries traffic for both VLAN *Marketing* and VLAN *Sales*.
- The trunk port on each Switch is tagged.
- The server connected to port 1 on Switch 1 has a NIC that supports 802.1Q tagging.
- The server connected to port 1 on Switch 1 is a member of both VLAN *Marketing* and VLAN *Sales*.
- All other stations use untagged traffic.

As data passes into the Switch, the Switch determines if the destination port requires the frames to be tagged or untagged. All traffic coming from and going to the server is tagged. Traffic coming from and going to the trunk ports is tagged. The traffic that comes from and goes to the other stations on this network is not tagged.

Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) traffic is always untagged and occurs on all ports when Spanning Tree is enabled.



*For the purposes of VLAN classification, packets arriving on a port with an 802.1Q tag containing a vlanid of 0 are treated as untagged.*

### **Mixing Port-based and Tagged VLANs**

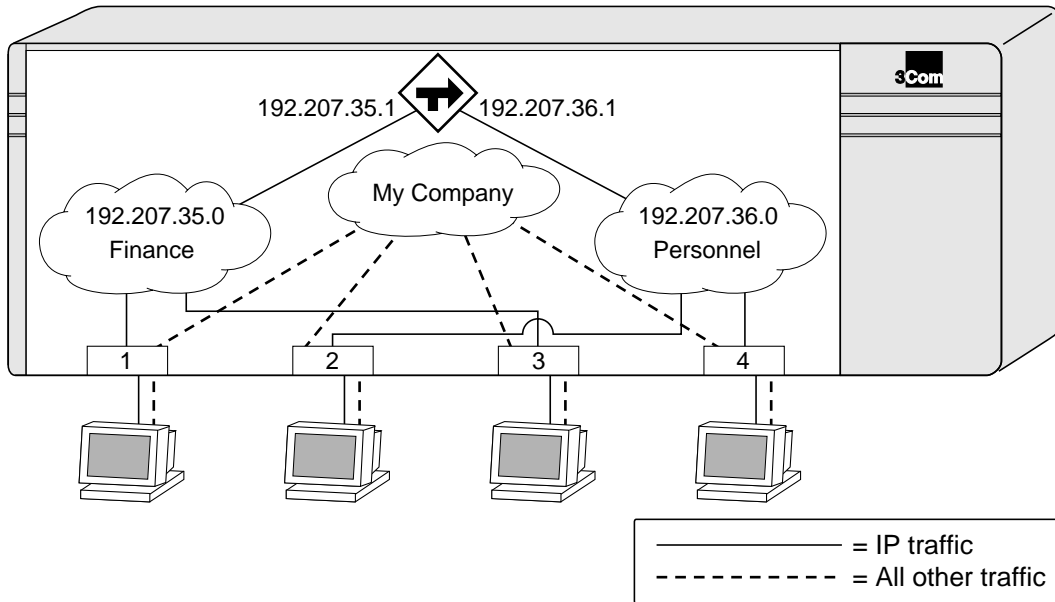
You can configure the Switch 9000 using a combination of port-based and tagged VLANs. A given port can be a member of multiple VLANs, with the stipulation that only one of its VLANs uses untagged traffic. In other words, a port can simultaneously be a member of one port-based VLAN and multiple tag-based VLANs.

### **Protocol-based VLANs**

Protocol-based VLANs enable you to define a protocol filter that the Switch 9000 uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.

Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols. For example, in Figure 5-6, the hosts are running both the IP and NetBIOS protocols.

The IP traffic has been divided into two IP subnets, 192.207.35.0 and 192.207.36.0. The subnets are internally routed by the Switch 9000. The subnets are assigned different VLAN names, *Finance* and *Personnel*, respectively. The remainder of the traffic belongs to the VLAN named *MyCompany*. All ports are members of the VLAN *MyCompany*.



**Figure 5-6** Protocol-based VLANs

### Predefined Protocol Filters

The following protocol filters are predefined on the Switch 9000:

- IP
- IPX
- NetBIOS
- DECNet

## Defining Protocol Filters

If necessary, you can define a customized protocol filter based on EtherType, LLC, and/or SNAP. Up to six filters may be part of a protocol filter. To define a protocol filter, do the following:

- Create a protocol using the following command:

```
create protocol <protocol_name>
```

- Configure the protocol using the following command:

```
config protocol <protocol_name> add <protocol_type>  
<hex_value>
```

Supported protocol types include:

- EtherType
- LLC
- SNAP

A maximum of seven protocol names, each containing a maximum of six protocol filters, can be defined.

## VLAN Names

The Switch 9000 supports up to 64 different VLANs. Each VLAN is given a name that can be up to 32 characters. VLAN names can use standard alpha-numeric characters. The following characters are not permitted in a VLAN name:

- Space
- Comma
- Quotation mark

VLAN names must begin with an alphabetical letter unless quotation marks are used to enclose a VLAN name that does not begin with an alphabetical character, or that contains a space, comma, or other special character.

VLAN names are locally significant. That is, VLAN names used on one Switch are only meaningful to that Switch. If another Switch is connected to it, the VLAN names have no significance to the other Switch.

### The Default VLAN

The Switch 9000 ships with one default VLAN that has the following properties:

- The VLAN name is *default*.
- It contains all the ports on a new or initialized Switch.
- The default VLAN is untagged, and has no VLANid or protocol filter assigned.

---

### Configuring VLANs on the Switch 9000

This section describes the commands associated with setting up VLANs on the Switch 9000. Configuring a VLAN involves the following steps:

- 1 Create and name the VLAN.
- 2 Assign an IP address and subnet mask (if applicable) to the VLAN, if needed.
- 3 Assign a VLANid, if any ports in this VLAN will use a tag.
- 4 Assign one or more ports to the VLAN.

As you add each port to the VLAN, decide if the port will use an 802.1Q tag.

Table 5-1 describes the commands used to configure a VLAN.

**Table 5-1** VLAN Configuration Commands

Command	Description
<code>create vlan &lt;name&gt;</code>	Allows you to create a named VLAN.
<code>create protocol &lt;protocol_name&gt;</code>	Allows you to create a user-defined protocol.
<code>config protocol &lt;protocol_name&gt; add &lt;protocol_type&gt; &lt;hex_value&gt;</code>	Allows you to configure a protocol filter. Supported protocol types include: <ul style="list-style-type: none"> <li>■ EtherType</li> <li>■ LLC</li> <li>■ SNAP</li> </ul>
<code>config vlan &lt;name&gt; ipaddress &lt;ipaddress&gt; {&lt;mask&gt;}</code>	Allows you to assign an IP address and an optional mask to the VLAN.
<code>config vlan &lt;name&gt; [add   delete] port &lt;portlist&gt; {tagged   untagged}</code>	Allows you to add and delete ports within the VLAN. You can specify tagged and untagged port(s). By default, ports are untagged.
<code>config vlan &lt;name&gt; protocol [&lt;protocol_name&gt;   any]</code>	Allows you to configure a protocol-based VLAN. If the keyword “any” is specified, then it becomes the default VLAN. All packets that cannot be classified into other protocol-based VLANs are assigned to the default VLAN of that port.
<code>config vlan &lt;name&gt; tag &lt;vlanid&gt;</code>	Allows you to assign a numerical VLANid. The valid range is from 1 to 4095.
<code>config dot1p ethertype &lt;ethertype&gt;</code>	Allows you to configure an IEEE 802.1Q Ethertype. Use this command if you have another switch that supports 802.1Q, but uses a different Ethertype. The default value used by the Switch is 8100.

### VLAN Configuration Examples

The following example creates a port-based VLAN named *accounting*, assigns the IP address 132.15.121.1, and assigns ports 1, 2, 3, and 6 to it:

```
create vlan accounting
config accounting ipaddress 132.15.121.1
config accounting add port 1-3,6
```



*Because VLAN names are unique, you do not need to enter the keyword “vlan” after you have created the unique VLAN name. You can use the VLAN name alone.*



The following example creates a tag-based VLAN named *video*. It assigns the VLANid 1000. Ports 4–8 are added as tagged ports to the VLAN.

```
create vlan video
config video tag 1000
config video add port 4-8 tagged
```

The following example creates a VLAN named *Sales*, with the VLANid 120. The VLAN uses both tagged and untagged ports. Ports 1–3 are tagged, and ports 4 and 7 are untagged. Note that when not explicitly specified, ports are added as untagged.

```
create vlan sales
config sales tag 120
config sales add port 1-3 tagged
config sales add port 4,7
```

The following example creates a protocol-based VLAN named *IPSales*. Ports 6 through 8 are assigned to the VLAN.

```
create vlan ipsales
config ipsales protocol ip
config ipsales add port 6-8
```

The following example defines a protocol filter, *myprotocol*, for the purposes of later applying to a VLAN. This is an example only, and has no real-world application.

```
create protocol myprotocol
config protocol myprotocol add etype 0xf0f0
config protocol myprotocol add etype 0xffff
```

---

## Displaying VLAN Settings

To display VLAN settings, use the following command:

```
show vlan {<name> | all}
```

The show command displays summary information about each VLAN, and includes the following:

- Name
- VLANid
- Ports assigned

- Status for each port
  - Enabled/disabled
  - Tagged/untagged
- Protocol information
- IP address
- STPD information

Sample output from this command is as follows:

```
3C16990:7 # sh vlan all
VLAN "Default" created by user
  Tagging:      802.1Q Tag 1
  IP:           192.207.37.214/255.255.255.0
  STPD: Domain "s0" is not running spanning tree protocol.
  Protocol:     Match all unfiltered protocols.
  Qos Profile:  QP1
  Ports:       16. (Number of active port=1)
  Untag:       3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
VLAN "green" created by user
  Tagging:      802.1Q Tag 11
  IP:           Not configured
  STPD: Domain "s0" is not running spanning tree protocol.
  Protocol:     Match all unfiltered protocols.
  Qos Profile:  QP1
  Ports:       3. (Number of active port=0)
  Untag:       1 2
  Tagged:      7
```

To display protocol information, use the following command:

```
show protocol {<protocol> | all}
```

Sample output from this command is as follows:

```
show protocol all
  Protocol Name      Type  Value
-----
IP                  etype 0x0806
                   etype 0x0800
ipx                  etype 0x8137
netbios              11c   0xf0f0
decnet               etype 0x6004
                   etype 0x6003
```

This show command displays protocol information, including the following:

- Protocol name
- List of protocol fields
- VLANs that use the protocol

---

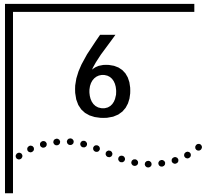
## Deleting and Resetting VLANs

To delete a VLAN, or to return VLAN settings to their defaults, use the commands listed in Table 5-2.

**Table 5-2** VLAN Delete and Reset Commands

Command	Description
<code>delete vlan &lt;name&gt;</code>	Allows you to remove a VLAN.
<code>delete protocol &lt;protocol&gt;</code>	Allows you to remove a protocol.
<code>unconfig vlan &lt;name&gt; ipaddress</code>	Allows you to remove the IP address.





# SWITCH FORWARDING DATABASE (FDB)

This chapter describes the contents of the Switch forwarding database (FDB), how the FDB works, and how to configure the FDB.

---

## Overview of the FDB

The Switch 9000 maintains a database of all addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered.

### FDB Contents

The database holds up to a maximum of 12,000 entries. Each entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all members of the VLAN.

### FDB Entry Types

The following are three types of entries in the FDB:

- **Dynamic entries** — Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (ageing time), the Switch has not received a frame containing that source address. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the Switch is reset or a power off/on cycle occurs.

For more information about setting the Ageing time, refer to “Configuring FDB Entries,” page 6-3.

- **Static entries** — If the ageing time is set to 00:00, all dynamic entries in the database are defined as non-ageing entries. This means that they do not age, but they are still deleted if the Switch is reset.

- **Permanent entries** — Permanent entries are retained in the database if the Switch is reset or a power off/on cycle occurs. The system administrator must make entries permanent. A permanent entry can either be a unicast or multicast MAC address. All entries entered by way of the command-line interface are stored as permanent. The Switch can support a maximum of 64 permanent entries.

**PACE Prioritization** For devices supporting PACE, the Switch 9000 can be configured to recognize PACE modified addresses. When present, the Switch assigns PACE traffic to the high priority queue within the switch.

Recognition of PACE traffic is controlled by the following commands:

```
enable pace
disable pace
```

### **How FDB Entries are Added**

Entries are added into the FDB in two ways:

- The Switch can learn entries. That is, the Switch updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received.
- You can enter and update entries using a MIB browser, an SNMP Network Manager, or the command-line interface, as described in the next section.

## Configuring FDB Entries

To configure entries in the FDB, use the commands listed in Table 6-1.

**Table 6-1** FDB Configuration Commands

Command	Description
<code>create fdbentry &lt;mac_address&gt; vlan &lt;name&gt; &lt;portlist&gt;</code>	<p>Allows you to create a permanent FDB entry. Specify the following:</p> <ul style="list-style-type: none"> <li>■ <code>mac_address</code> — device MAC address, using colon separated bytes</li> <li>■ <code>name</code> — VLAN associated with MAC address</li> <li>■ <code>portlist</code> — port number associated with MAC address</li> </ul> <p>If more than one port number is associated with a permanent MAC entry, packets will be multicast to the multiple destinations.</p>
<code>config fdb agingtime &lt;delay&gt;</code>	<p>Allows you to configure the FDB ageing time. The range is 15 through 1,000,000 seconds. The default value is 1800 seconds. A value of 0 indicates that the entry should never be aged out.</p>

### FDB Configuration Example

This example adds a permanent entry to the FDB:

```
create fdbentry 02:60:8c:12:34:56 vlan marketing port 4
```

The permanent entry has the following characteristics:

- MAC address is 02608c123456
- VLAN name is marketing
- Port number for this device is 4

## Displaying FDB Entries

To display FDB entries, use the command:

```
show fdb {all | <mac_address> | vlan <name> | <portlist> | permanent}
```

Where:

- **all** — displays all FDB entries
- **mac\_address** — displays the entry for a particular MAC address
- **vlan <name>** — displays the entries for a VLAN

- **portlist** — displays the entries for one or more ports
- **permanent** — displays all permanent entries

The following sample output shows the information displayed when you request output for all FDB entries:

```
show fdb
```

```

Hash  Num      Mac              Vlan          Flags  Ptag  Portlist
-----
0f00: 0  ff:ff:ff:ff:ff:ff  Default(0001) sm  0fef  CPU
3289: 0  00:e0:2b:00:00:00  Default(0001) sm  0ffb  CPU
373d: 0  01:80:c2:00:00:00          (0000) sm  0ffb  CPU
72f3: 0  00:e0:2b:00:a4:00  Default(0001) sm  0ff1  CPU
Total: 4 Static: 4 Perm: 0 Dyn: 0 Dropped: 0
FDB Aging time: 300

```

The show command displays summary information, including

- MAC address
- VLAN name and VLANid
- Entry method (dynamic/static/permanent)
- Port

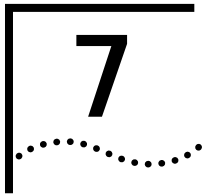
## Removing FDB Entries

You can remove one or more specific entries from the FDB, or you can clear the entire FDB of all entries by using the commands listed in Table 6-2.

**Table 6-2** Removing FDB Entry Commands

Command	Description
<code>delete fdbentry &lt;mac_address&gt; vlan &lt;name&gt;</code>	Allows you to delete a permanent FDB entry.
<code>clear fdb {all   &lt;mac_address&gt;   vlan &lt;name&gt;   &lt;portlist&gt;}</code>	Allows you to clear dynamic FDB entries that match the filter. Use the keyword "all" to clear all dynamic entries.





# SPANNING TREE PROTOCOL (STP)

Using the Spanning Tree Protocol (STP) functionality of the Switch 9000 makes your network more fault tolerant.

The following sections describe STP concepts, and how STP features are supported by the Switch.



*STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the Switch 9000 will be defined as a bridge.*

---

## Overview of the Spanning Tree Protocol

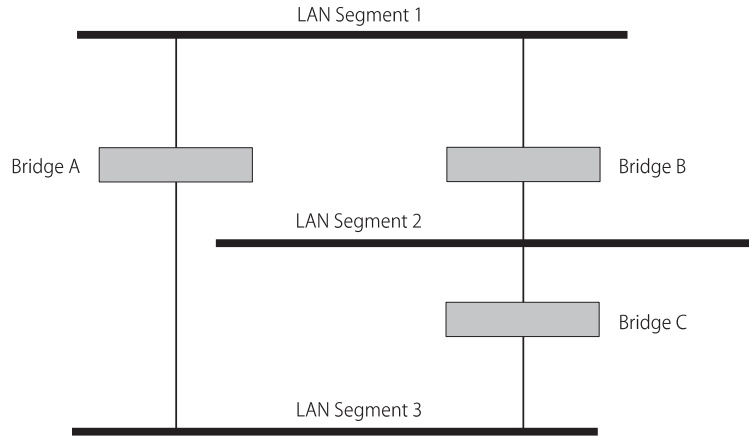
STP is a bridge-based mechanism for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational
- Redundant paths are enabled if the main path fails



**CAUTION:** *You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.*

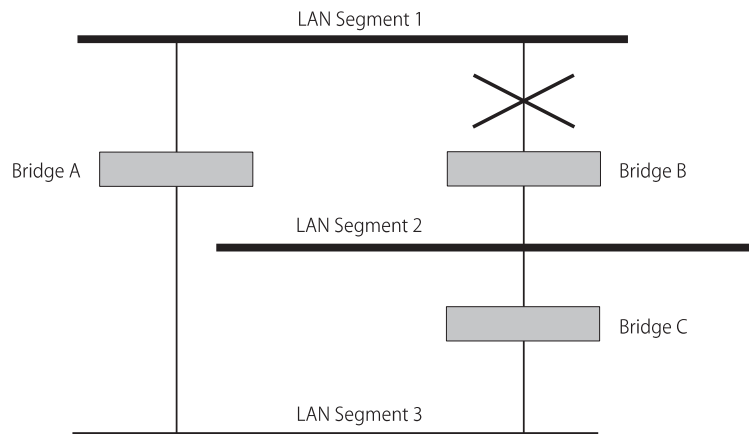
Figure 7-1 shows a network containing three LAN segments separated by three bridges. Using this configuration, each segment can communicate with the others by using two paths.



**Figure 7-1** Network with an illegal topology

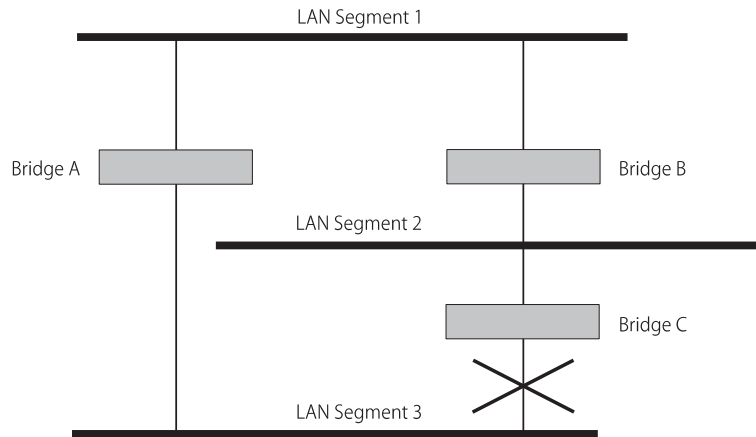
This configuration is illegal because it creates loops that cause the network to overload. However, STP allows you to use this configuration because STP detects duplicate paths and immediately prevents (or *blocks*) one of them from forwarding traffic.

Figure 7-2 shows an example of enabling STP on the bridges in the configuration. The STP system has decided that traffic from LAN segment 2 to LAN segment 1 can only flow through Bridges C and A.



**Figure 7-2** Traffic flowing through Bridges C and A

If the link through Bridge C fails, as shown in Figure 7-3, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.



**Figure 7-3** Traffic flowing through Bridge B

**How STP Works** STP has the following three stages of operation:

- Initialization
- Stabilization
- Reconfiguration

### Initialization

Initially, the STP system requires the following before it can configure the network:

- All bridges exchange information by way of Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address
- To determine a single root bridge as a result of BPDU exchange

The Root Bridge is selected on the basis of it having the lowest Bridge Identifier value. This value is a combination of the unique MAC address of the bridge and a priority component defined for the bridge.

The Root Bridge generates BPDUs on all ports at a regular interval known as the Hello Time. All other bridges in the network have a Root Port. This is the port that costs the least in getting to the Root Bridge, and it is used for receiving the BPDUs initiated by the Root Bridge.

### Stabilization

After all bridges on the network have determined the configuration of their ports, each bridge only forwards traffic between the Root Port and the ports that are the Designated Bridge Ports for each network segment to which they are attached. All other ports are *blocked*, which means that they are prevented from forwarding traffic.

### Reconfiguration

In the event of a network failure (such as a segment going down) the STP system reconfigures the network to adjust for the changes. If the topology of the network changes, the Root Bridge sends out an SNMP trap.

---

## Spanning Tree Domains

The Switch 9000 can be partitioned into multiple virtual bridges. Each virtual bridge can run an independent spanning tree instance. Each spanning tree instance is called a *Spanning Tree Domain* (STPD). Each STPD has its own Root Bridge and active path. Once the STPD is created, one or more VLANs can be assigned to it.

A port can belong to only one STPD. If a port is a member of multiple VLANs, then all those VLANs must belong to the same STPD.

The key points to remember when configuring VLANs and STP are the following:

- Each VLAN forms an independent broadcast domain.
- STP blocks paths to create a loop-free environment.
- When STP blocks a path, no data can be transmitted or received on the blocked port.

- Within any given STPD, all VLANs belonging to it use the same spanning tree.



*Care must be taken to ensure that STPD instances within a single Switch do not see each other in the same broadcast domain. This could happen if, for example, another external bridge is used to connect VLANs belonging to separate STPDs.*

**Defaults** The default device configuration contains a single STPD called *s0*. The default VLAN is a member of STPD *s0*.

All STP parameters default to the IEEE 802.1D values, as appropriate.

## STP Configurations

When you assign VLANs to an STPD, pay careful attention to the STP configuration and its effect on the forwarding of VLAN traffic.

Figure 7-4 illustrates a network that uses VLAN tagging for trunk connections. The following four VLANs have been defined:

- *Sales* is defined on Switch A, Switch B, and Switch M.
- *Personnel* is defined on Switch A, Switch B, and Switch M.
- *Manufacturing* is defined on Switch Y, Switch Z, and Switch M.
- *Engineering* is defined on Switch Y, Switch Z, and Switch M.
- *Marketing* is defined on all Switches (Switch A, Switch B, Switch Y, Switch Z, and Switch M).

Two STPDs are defined:

- STPD1 contains VLANs *Sales* and *Personnel*.
- STPD2 contains VLANs *Manufacturing* and *Engineering*.

The VLAN *Marketing* is not assigned to a STPD.

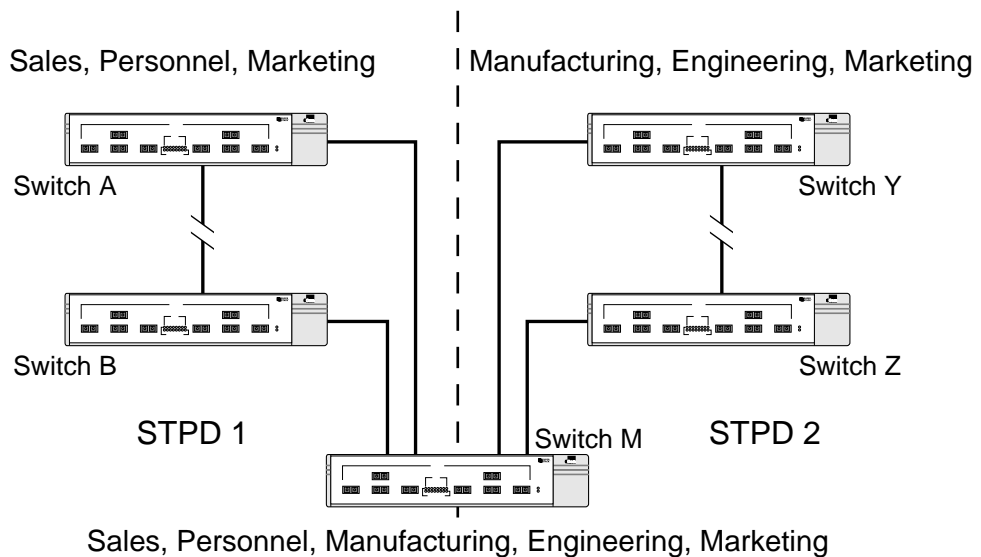


Figure 7-4 Multiple Spanning Tree Domains

When the Switches in this configuration start up, STP configures each STP domain such that there are no active loops in the topology. STP could configure the topology in a number of ways to make it loop-free.

In Figure 7-4, the connection between Switch A and Switch B is put into blocking state, and the connection between Switch Y and Switch Z is put into blocking state. After STP converges, all the VLANs can communicate, and all bridging loops are prevented.

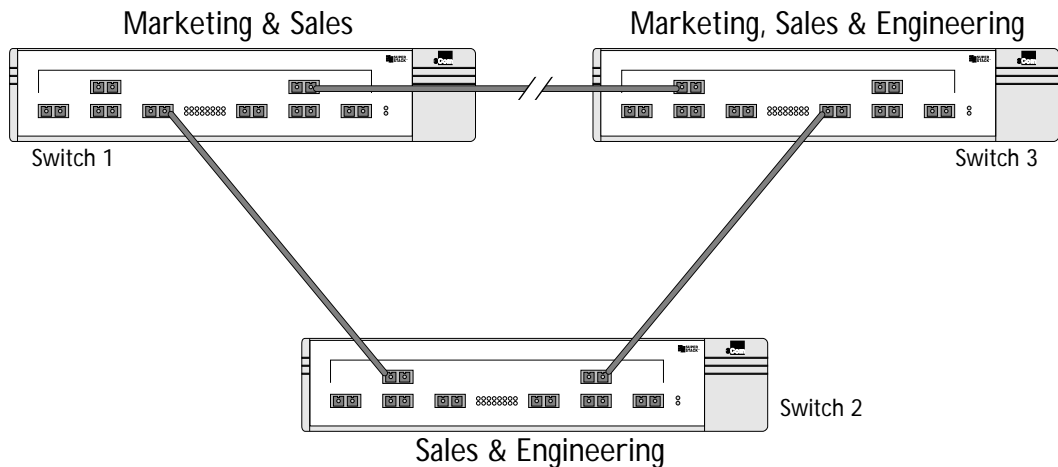
The VLAN *Marketing*, which has not been assigned to any STPD, communicates using all five Switches. The topology has no loops, because STP has already blocked the port connection between Switch A and Switch B, and between Switch Y and Switch Z.

## STP Configurations to Avoid

Within a single STPD, you must be careful when configuring your VLANs. The following figures illustrate networks that have been *incorrectly* set up so that the STP configuration disables the ability of the Switches to forward VLAN traffic.

The tag-based network in Figure 7-5 has the following configuration:

- Switch 1 contains VLAN *Marketing* and VLAN *Sales*.
- Switch 2 contains VLAN *Engineering* and VLAN *Sales*.
- Switch 3 contains VLAN *Marketing*, VLAN *Engineering*, and VLAN *Sales*.
- The tagged trunk connections for three Switches form a triangular loop that is not permitted in an STP topology.
- All VLANs in each switch are members of the same STPD.



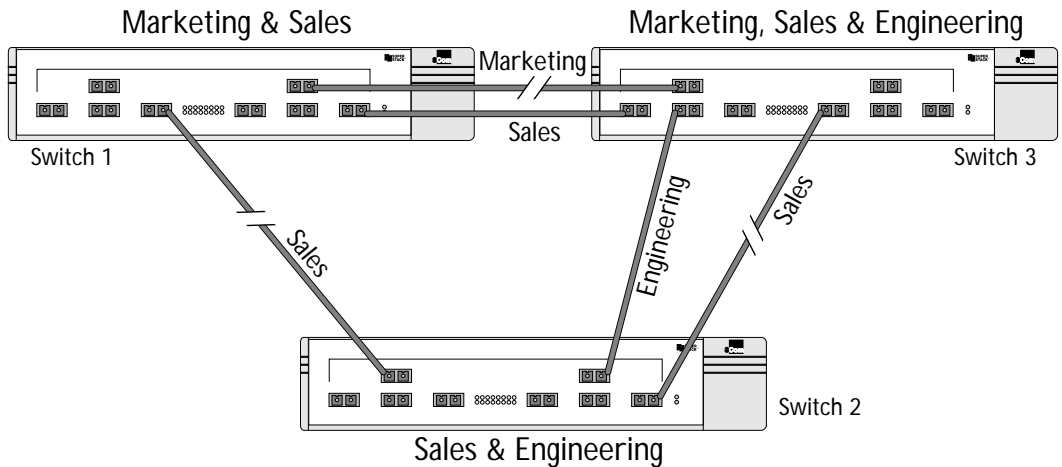
**Figure 7-5** Tag-based STP configuration

STP may block traffic between Switch 1 and Switch 3 by disabling the trunk ports for that connection on each Switch.

Switch 2 has no ports assigned to VLAN *Marketing*. Therefore, if the trunk for VLAN *Marketing* on Switches 1 and 3 is blocked, the traffic for VLAN *Marketing* will not be able to traverse the Switches.



Figure 7-6 shows a similar configuration in which the VLANs are all port-based. The trunk connections between the Switches require one trunk port per Switch for each VLAN.



**Figure 7-6** Port-based STP configuration

To remove all the bridging loops, STP may block traffic on the VLAN *Sales* trunk between Switch 1 and Switch 2, on the VLAN *Sales* trunk between Switch 2 and Switch 3, and on the VLAN *Marketing* trunk between Switch 1 and Switch 3.

Of the three VLANs, only VLAN *Engineering* is correctly configured, so that all ports in that VLAN can communicate with each other.

## Creating STP Domains

To create one or more STP domains on your Switch, use the following command at the administrator prompt:

```
create stpd <stpd_name>
```



*STPD and VLAN profile names must all be unique. For example, a name given to identify a VLAN cannot be used when you create an STPD.*

To add one or more VLANs to the STPD, use the following command:

```
config stpd <stpd_name> add vlan <name>
```

## Enabling STP on the Switch

To enable STP for one or more STP domains on your Switch, use the following command at the administrator prompt:

```
enable stpd [<stpd_name> | all]
```

## Configuring STP

You can configure the following STP parameters for each STPD on the Switch:

- Hello Time
- Forward Delay
- Max Age
- Bridge Priority

You can configure the following STP parameters for each port on the Switch:

- Path Cost
- Port Priority



**CAUTION:** You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

Table 7-1 shows the commands used to configure STP.

**Table 7-1** STP Configuration Commands

Command	Description
<code>create stpd &lt;stpd_name&gt;</code>	Allows you to create an STPD. When created, an STPD has the following default parameters: <ul style="list-style-type: none"> <li>■ Bridge priority — 32,768</li> <li>■ Hello time — 2 seconds</li> <li>■ Forward delay — 15 seconds</li> </ul>
<code>enable stpd [&lt;stpd_name&gt;   all]</code>	Allows you to enable STP for one or more STPDs. The default setting is disabled.
<code>enable stpd port &lt;portlist&gt;</code>	Allows you to enable STP on one or more ports.
<code>config stpd &lt;stpd_name&gt; add vlan &lt;name&gt;</code>	Allows you to add a VLAN to the STPD.
(continued)	

**Table 7-1** STP Configuration Commands (continued)

Command	Description
<code>config stpd &lt;stpd_name&gt; delete vlan [&lt;name&gt;   all]</code>	Allows you to remove one or all VLANs from an STPD. If all is specified, the association between the STPD and VLAN is removed, but both still exist.
<code>config stpd &lt;stpd_name&gt; hellotime &lt;value&gt;</code>	Allows you to specify the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge.  The range is 1 through 10. The default setting is 2 seconds.
<code>config stpd &lt;stpd_name&gt; forwarddelay &lt;value&gt;</code>	Allows you to specify the time (in seconds) that the ports on this STPD spend in the listening and learning states when the Switch is the Root Bridge.  The range is 4 through 30. The default setting is 15 seconds.
<code>config stpd &lt;stpd_name&gt; maxage &lt;value&gt;</code>	Allows you to specify the maximum age of a BPDU in this STPD.  The range is 6 through 40. The default setting is 20 seconds.  Note that the time must be greater than, or equal to $2 \times (\text{Hello Time} + 1)$ and less than, or equal to $2 \times (\text{Forward Delay} - 1)$ .
<code>config stpd &lt;stpd_name&gt; priority &lt;value&gt;</code>	Allows you to specify the priority of the STPD. By changing the priority of the Switch, you can make it more or less likely to become the Root Bridge.  The range is 0–65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.
<code>config stpd &lt;stpd_name&gt; port cost &lt;value&gt; &lt;portlist&gt;</code>	Allows you to specify the path cost of the port in this STPD.  The range is 1–65,535. The Switch automatically assigns a default path cost based on the speed of the port, as follows: <ul style="list-style-type: none"> <li>■ For a 10Mbps port, the default cost is 100.</li> <li>■ For a 100Mbps port, the default cost is 19.</li> <li>■ For a 1000Mbps port, the default cost is 4.</li> </ul>
<code>config stpd &lt;stpd_name&gt; port priority &lt;value&gt; &lt;portlist&gt;</code>	Allows you to specify the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the Root Port.  The range is 0–255. The default setting is 128. A setting of 0 indicates the lowest priority.

**Configuration Example**

The following example creates and enables an STPD named *Backbone\_st*. It assigns the *Manufacturing* VLAN to the STPD. It disables STP on ports 1 through 3, and port 4.

```
create stpd backbone_st
config stpd backbone_st add vlan manufacturing
enable stpd backbone_st
disable stpd backbone_st port 1-3,4
```

---

**Displaying STP Settings**

To display STP settings, use the following command:

```
show stpd {<stpd_name> | all}
```

This command displays the following information:

- STPD name
- Bridge ID
- STPD configuration information

Sample output from the command is displayed below:

```
show stpd
```

```
Stpd:s0                Stp:DISABLED          Number of Ports:8
Ports: 1,2,3,4,5,6,7,8
Vlans:  Default
BridgeID                80:00:00:e0:2b:00:a4:00
Designated root:       00:00:00:00:00:00:00:00
RootPathCost: 0
MaxAge: 0s              HelloTime: 0s         ForwardDelay: 0s
CfgBrMaxAge: 20s       CfgBrHelloTime: 2s   CfgBrForwardDelay:15s
Topology Change Time: 35s           Hold time: 1s
Topology Change Detected: FALSE      Topology Change:FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 0s
```

To display port-specific STP information, use the following command:

```
show stpd <stpd_name> port <portlist>
```

This command displays the following:

- STPD port configuration
- STPD state (root bridge, and so on)
- STPD port state (forwarding, blocking, and so on)

Sample output from the command is as follows:

```
3C16990:28 # sh stpd s0 po 5-8
```

```
Stpd: s0 Port: 8 PortId: 8008 Stp: ENABLED Path Cost: 4
Port State: FORWARDING Topology Change Ack: FALSE
Port Priority: 128
Designated Root: 80:00:08:00:4e:2c:13:00 Designated Cost: 0
Designated Bridge: 80:00:08:00:4e:2c:13:00
Designated Port Id: 8008
```

```
Stpd: s0 Port: 7 PortId: 8007 Stp: ENABLED Path Cost: 4
Port State: FORWARDING Topology Change Ack: FALSE
Port Priority: 128
Designated Root: 80:00:08:00:4e:2c:13:00 Designated Cost: 0
Designated Bridge: 80:00:08:00:4e:2c:13:00
Designated Port Id: 8007
```

```
Stpd: s0 Port: 6 PortId: 8006 Stp: ENABLED Path Cost: 4
Port State: BLOCKING Topology Change Ack: FALSE
Port Priority: 128
Designated Root: 80:00:08:00:4e:2c:13:00 Designated Cost: 0
Designated Bridge: 80:00:08:00:4e:2c:13:00
Designated Port Id: 8003
```

```
Stpd: s0 Port: 5 PortId: 8005 Stp: ENABLED Path Cost: 4
Port State: FORWARDING Topology Change Ack: FALSE
Port Priority: 128
Designated Root: 80:00:08:00:4e:2c:13:00 Designated Cost: 0
Designated Bridge: 80:00:08:00:4e:2c:13:00
Designated Port Id: 8005
```

```
* 3C16990:29 #
```

## Disabling and Resetting STP

To disable STP or return STP settings to their defaults, use the commands listed in Table 7-2.

**Table 7-2** STP Disable and Reset Commands

Command	Description
<code>delete stpd &lt;stpd_name&gt;</code>	Allows you to remove an STPD. An STPD can only be removed if all VLANs have been deleted from it.
<code>disable stpd [&lt;stpd_name&gt;   all]</code>	Allows you to disable the STP mechanism on one or all STPDs.
<code>disable stpd port &lt;portlist&gt;</code>	Allows you to disable STP on one or more ports.
<code>unconfig stpd {&lt;stpd_name&gt;   all}</code>	Allows you to restore default STP values to one or all STPDs.



**CAUTION:** *If you ignore warnings and delete an STPD without removing all of its VLAN members first, those VLANs will also be deleted.*

# 8

## IP UNICAST ROUTING

This chapter describes how to configure IP routing on the Switch 9000. It assumes that you are already familiar with IP unicast routing. If not, refer to the following publications for additional information:

RFC 1058 — *Routing Information Protocol*

RFC 1256 — *ICMP Router Discovery Messages*

RFC 1723 — *RIP Version 2*

RFC 1812 — *Requirements for IP Version 4 Routers*

---

### Overview of IP Unicast Routing

The Switch 9000 provides full Layer 3, IP unicast routing. It exchanges routing information with other routers on the network using the Routing Information Protocol (RIP). The Switch 9000 dynamically builds and maintains a routing table, and determines the best path for each of its routes.

Each host using the IP unicast routing functionality of the Switch 9000 must have a unique IP address assigned. In addition, the default gateway assigned to the host must be the IP address of the Switch 9000 router interface.

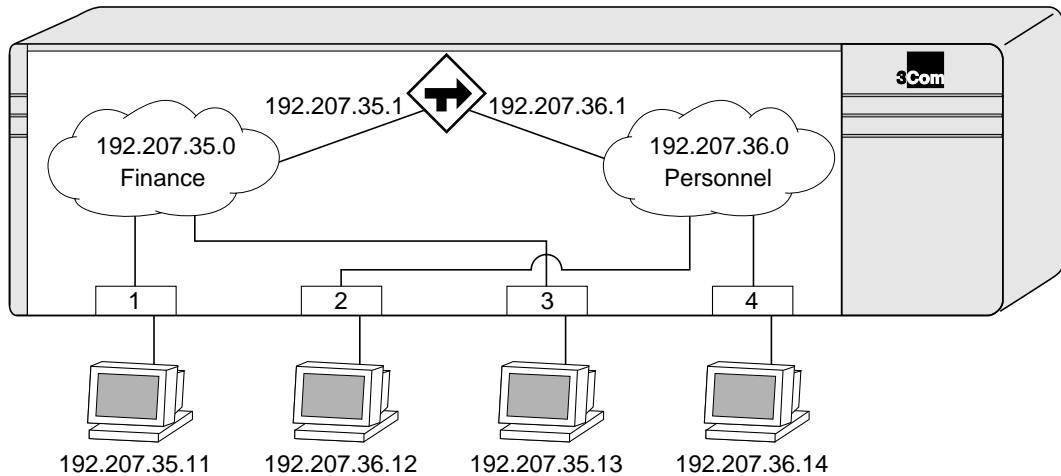
### Router Interfaces

The routing software and hardware routes IP traffic between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to route between the VLANs. Both the VLAN switching and IP routing function occur within the Switch 9000.

In Figure 8-1, a Switch 9000 is shown with two VLANs defined: *Finance* and *Personnel*. Ports 1 and 3 are assigned to *Finance*; ports 2 and 4 are assigned to *Personnel*. *Finance* belongs to the IP network 192.207.35.0;

the router interface for *Finance* is assigned the IP address 192.206.35.1. *Personnel* belongs to the IP network 192.207.36.0; its router interface is assigned IP address 192.207.36.1. Traffic within each VLAN is switched using the Ethernet MAC addresses. Traffic between the two VLANs is routed using the IP addresses.



**Figure 8-1** Routing between VLANs

### Populating the Routing Table

The Switch 9000 maintains an IP routing table for both network routes and host routes. The table is populated from the following sources:

- Dynamically, by way of RIP packets or ICMP redirects exchanged with other routers
- Statically, by way of routes entered by the administrator
  - Default routes, configured by the administrator
  - Locally, by way of interface addresses assigned to the Switch 9000
  - By other static routes, as configured by the administrator



## Dynamic Routes

Dynamic routes are typically learned by way of RIP. Routers using RIP exchange information in their routing tables in the form of RIP advertisements. Using dynamic routes, the routing table contains only networks that are reachable.

Dynamic routes are aged out of the table when a RIP update for the network is not received for a period of time.

## Static Routes

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure up to 64 static unicast routes on the Switch 9000.

Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised by using the following command:

```
[enable | disable] rip exportstatic
```

The default setting is enabled. Static routes are never aged out of the routing table.

## Multiple Routes

When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask. If these are still equal, the router picks the route using the following criteria (in the order specified):

- Directly attached network interfaces
- ICMP redirects (refer to Table 8-4)
- Static routes
- RIP
- Directly attached network interfaces that are not active.

You can also configure *blackhole* routes—traffic to these destinations is silently dropped.

---

## Configuring IP Unicast Routing

This section describes the commands associated with configuring IP unicast routing on the Switch 9000. Configuring routing involves the following steps:

- Verify the Switch operating mode is set to `iprouting`, by using the following command:

```
show switch
```

If it is not, use the following command:

```
config devicemode iprouting
```

- Create and configure two or more VLANs.

For information on creating and configuring VLANs, refer to Chapter 5.

- Assign each VLAN that will be using routing an IP address, using the following command:

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```

Ensure that each VLAN has a unique IP address.

- Configure a default route, using the following command:

```
config iproute add default <gateway> {<metric>}
```

Default routes are used when the router has no other dynamic or static route to the requested destination.

- Turn on IP routing for one or more VLANs, using the following command:

```
enable ipforwarding {vlan <name> | all}
```

- Turn on RIP, using the following command:

```
enable rip
```

When you create a VLAN, RIP is enabled by default. You must, however, enable RIP on the Switch to route traffic. To disable RIP on a particular VLAN, use the following command:

```
- config rip delete {vlan <name>}
```

---

## Verifying the IP Unicast Routing Configuration

Use the `show iproute` command to display the current configuration of IP unicast routing for the Switch, and for each VLAN. The `show iproute` command displays the currently configured routes, including how each route was learned.

Additional verification commands include:

- `show iparp`

Displays the IP ARP table of the switch.

- `show ipfdb`

Displays the hosts that have been transmitting or have received packets, as well as the port and VLAN for each host.

---

## Configuring DHCP/BOOTP Relay

Once IP unicast routing is configured, you can configure the Switch 9000 to forward HP or BOOTP requests coming from clients on subnets being serviced by the Switch 9000 and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, do the following:

- 1 Configure VLANs and IP unicast routing.
- 2 Enable the DHCP or BOOTP relay function, using the following command:

```
enable bootprelay
```

- 3 Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

```
config bootprelay add <ipaddress>
```

- 4 To delete an entry, use the following command:

```
config bootprelay delete {<ipaddress> | all}
```

## Verifying the DHCP/BOOTP Relay Configuration

To verify the DHCP/BOOTP relay configuration, use the following command:

```
show ipconfig
```

This command displays the configuration of the BOOTP relay service, and the addresses that are currently configured.

Table 8-1 describes the commands used to configure basic IP settings on the Switch.

**Table 8-1** Basic IP Commands

Command	Description
<code>enable bootp {vlan &lt;name&gt;   all}</code>	Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server. The default setting is enabled for all VLANs.
<code>enable bootprelay</code>	Enables the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests.
<code>enable ipforwarding {vlan &lt;name&gt;   all}</code>	Enables IP routing for one or more VLANs. If no argument is provided, enables routing for all VLANs that have been configured with an IP address. The default setting for ipforwarding is disabled.
<code>enable ipforwarding broadcast {vlan &lt;name&gt;   all}</code>	Enables forwarding IP broadcast traffic for one or more VLANs. If no argument is provided, enables broadcast forwarding for all VLANs. To enable, ipforwarding must be enabled on the VLAN. The default setting is enabled.
<code>config bootprelay add &lt;ipaddress&gt;</code>	Adds the IP destination address to forward BOOTP packets.
<code>config bootprelay delete [&lt;ipaddress&gt;   all]</code>	Removes one or all IP destination addresses for forwarding BOOTP packets.
<code>config iparp add &lt;ipaddress&gt; &lt;mac_address&gt;</code>	Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.
<code>config iparp delete &lt;ipaddress&gt;</code>	Deletes an entry from the ARP table. Specify the IP address of the entry.
<code>disable bootp vlan [&lt;name&gt;   all]</code>	Disables the generation and processing of BOOTP packets.
<code>disable bootprelay</code>	Disables the forwarding of BOOTP requests.
<code>disable ipforwarding {vlan &lt;name&gt;   all}</code>	Disables routing for one or more VLANs.
<code>disable ipforwarding broadcast {vlan &lt;name&gt;   all}</code>	Disables routing of broadcasts to other networks.
<code>clear iparp [&lt;ipaddress&gt;   vlan &lt;name&gt;   all]</code>	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.

(continued)

**Table 8-1** Basic IP Commands (continued)

Command	Description
<code>clear ipfdb [&lt;ipaddress&gt;   vlan &lt;name&gt;   all]</code>	Removes the dynamic entries in the IP forwarding database.

Table 8-2 describes the commands used to configure the IP route table.

**Table 8-2** Route Table Configuration Commands

Command	Description
<code>config iproute add &lt;ipaddress&gt; &lt;mask&gt; &lt;gateway&gt; {&lt;metric&gt;}</code>	Adds a static address to the routing table. Use a value of 255.255.255.255 for <code>mask</code> to indicate a host entry.
<code>config iproute delete &lt;ipaddress&gt; &lt;mask&gt; &lt;gateway&gt;</code>	Deletes a static address from the routing table.
<code>config iproute add blackhole &lt;ipaddress&gt; &lt;mask&gt;</code>	Adds a blackhole address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.
<code>config iproute delete blackhole &lt;ipaddress&gt; &lt;mask&gt;</code>	Deletes a blackhole address from the routing table.
<code>config iproute add default &lt;gateway&gt; {&lt;metric&gt;}</code>	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface. If no metric is specified, the default metric of 1 is used.
<code>config iproute delete default &lt;gateway&gt;</code>	Deletes a default gateway from the routing table.

Table 8-3 describes the commands used to configure RIP.

**Table 8-3** RIP Configuration Commands

Command	Description
<code>enable rip</code>	Enables RIP. The default setting is disabled.
<code>enable rip aggregation</code>	Enables RIP aggregation of subnet information on a RIP version 2 interface. The default setting is enabled.
<code>enable rip exportstatic</code>	Enables the advertisement of static routes using RIP. The default setting is enabled.
<code>enable rip poisonreverse</code>	Enables the split horizon with poison-reverse algorithm for RIP. The default setting is enabled.

(continued)

**Table 8-3** RIP Configuration Commands (continued)

Command	Description
<code>enable rip splithorizon</code>	Enables the split horizon algorithm for RIP. Default setting is enabled.
<code>enable rip triggerupdate</code>	Enables triggered updates. <i>Triggered updates</i> are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
<code>config rip add {vlan &lt;name&gt;   all}</code>	Configures RIP on an IP interface. If no VLAN is specified, then all is assumed. When an IP interface is created, per interface RIP configuration is enabled by default.
<code>config rip delete {vlan &lt;name&gt;   all}</code>	Disables RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
<code>config rip garbagetime {&lt;delay&gt;}</code>	Configures the RIP garbage time. The default setting is 120 seconds.
<code>config rip routetimeout {&lt;delay&gt;}</code>	Configures the route timeout. The default setting is 180 seconds.
<code>config rip rxmode [none   v1only   v2only   any] {vlan &lt;name&gt;   all}</code>	Changes the RIP receive mode for one or more VLANs. Specify: <ul style="list-style-type: none"> <li>■ none — Drop all received RIP packets.</li> <li>■ v1only — Accept only RIP version 1 format packets.</li> <li>■ v2only — Accept only RIP version 2 format packets.</li> <li>■ any — Accept both version 1 and version 2 packets.</li> </ul> If no VLAN is specified, the setting is applied to all VLANs. The default setting is "any".
<code>config rip txmode [none   v1only   v1comp   v2only] {vlan &lt;name&gt;   all}</code>	Changes the RIP transmission mode for one or more VLANs. Specify: <ul style="list-style-type: none"> <li>■ none — Do not transmit any packets on this interface.</li> <li>■ v1only — Transmit RIP version 1 format packets to the broadcast address.</li> <li>■ v1comp — Transmit version 2 format packets to the broadcast address.</li> <li>■ v2only — Transmit version 2 format packets to the RIP multicast address</li> </ul> If no VLAN is specified, the setting is applied to all VLANs. The default setting is "v2only".
<code>config rip updatetime {&lt;delay&gt;}</code>	Changes the periodic RIP update timer. The default setting is 30 seconds.
<code>disable rip</code>	Disables RIP.
<code>disable rip aggregation</code>	Disables the RIP aggregation of subnet information on a RIP version 2 interface.

(continued)

**Table 8-3** RIP Configuration Commands (continued)

Command	Description
<code>disable rip splithorizon</code>	Disables split horizon.
<code>disable rip poisonreverse</code>	Disables poison reverse.
<code>disable rip triggerupdate</code>	Disables triggered updates
<code>disable rip exportstatic</code>	Disables the filtering of static routes.
<code>unconfig rip {vlan &lt;name&gt;   all}</code>	Resets all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.

Table 8-4 describes the commands used to configure the ICMP protocol.

**Table 8-4** ICMP Configuration Commands

Command	Description
<code>enable icmp redirects {vlan &lt;name&gt;   all}</code>	Enables generation of ICMP redirect messages on one or more VLANs. The default setting is enabled.
<code>enable icmp unreachable {vlan &lt;name&gt;   all}</code>	Enables the generation of ICMP unreachable messages on one or more VLANs. The default setting is enabled.
<code>enable icmp userredirects</code>	Enables the modification of route table information when an ICMP redirect message is received. The default setting is disabled.
<code>enable irdp {vlan &lt;name&gt;   all}</code>	Enables the generation of ICMP router advertisement messages on one or more VLANs. The default setting is enabled.
<code>config irdp [multicast   broadcast]</code>	Configures the destination address of the router advertisement messages. The default setting is broadcast.
<code>config irdp &lt;mininterval&gt; &lt;maxinterval&gt; &lt;lifetime&gt; &lt;preference&gt;</code>	Configures the router advertisement message timers, using seconds. Specify: <ul style="list-style-type: none"> <li>■ <code>mininterval</code> — The minimum amount of time between router advertisements. The default setting is 450 seconds.</li> <li>■ <code>maxinterval</code> — The maximum time between router advertisements. The default setting is 600 seconds.</li> <li>■ <code>lifetime</code> — The default setting is 1,800 seconds.</li> <li>■ <code>preference</code> — The preference level of the router. An IRDP client always uses the router with the highest preference level. Change this setting to encourage or discourage the use of this router. The default setting is 0.</li> </ul>
<code>unconfig icmp</code>	Resets all ICMP settings to the default values.

(continued)

**Table 8-4** ICMP Configuration Commands (continued)

Command	Description
<code>unconfig irdp</code>	Resets all router advertisement settings to the default values.
<code>disable icmp redirects {vlan &lt;name&gt;   all}</code>	Disables the generation of ICMP redirects on one or more VLANs.
<code>disable icmp unreachable</code>	Disables the generation of ICMP unreachable messages on one or more VLANs.
<code>disable icmp useredirects</code>	Disables the changing of routing table information when an ICMP redirect message is received.
<code>disable irdp {vlan &lt;name&gt;   all}</code>	Disables the generation of router advertisement messages on one or more VLANs.

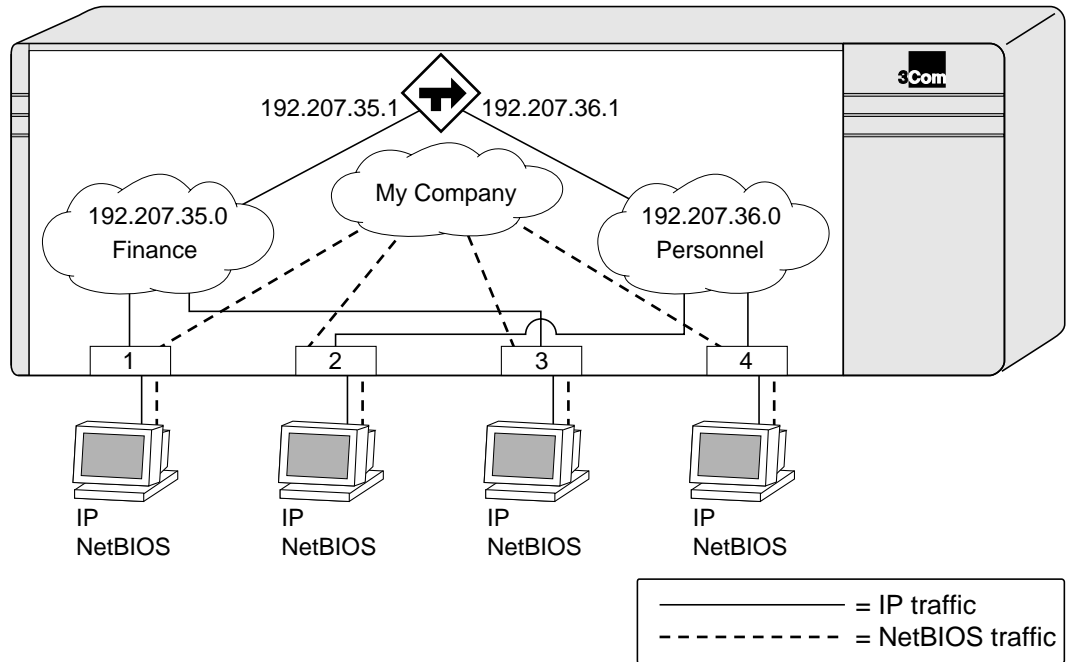
## Routing Configuration Example

Figure 8-2 illustrates a Switch that has three VLANs defined as follows:

- *Finance*
  - Protocol-sensitive VLAN using the IP protocol
  - Ports 1 and 3 have been assigned
  - IP address 192.207.35.1
- *Personnel*
  - Protocol-sensitive VLAN using the IP protocol
  - Ports 2 and 4 have been assigned
  - IP address 192.207.36.1
- *MyCompany*
  - Port-based VLAN
  - All ports have been assigned

The stations connected to ports 1 through 4 generate a combination of IP traffic and NetBIOS traffic. The IP traffic is filtered by the protocol-sensitive VLANs. All other traffic is directed to the VLAN *MyCompany*.





**Figure 8-2** Unicast Routing Configuration Example

In this configuration, all IP traffic from stations connected to ports 1 and 3 have access to the router by way of the VLAN *Finance*. Ports 2 and 4 reach the router by way of the VLAN *Personnel*. All other traffic (NetBIOS) is part of the VLAN *MyCompany*.

The example in Figure 8-2 is configured as follows:

```

create vlan Finance
create vlan Personnel
create vlan MyCompany

config Finance protocol ip
config Personnel protocol ip

config Finance add port 1,3
config Personnel add port 2,4
config MyCompany add port all

config Finance ipaddress 192.207.35.1
config Personnel ipaddress 192.207.36.1

enable ipforwarding
enable rip
    
```

## Displaying Router Settings

To display settings for various IP routing components, use the commands listed in Table 8-5.

**Table 8-5** Router Show Commands

Command	Description
<code>show ip config {vlan &lt;name&gt;   all}</code>	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none"> <li>■ IP address, subnet mask</li> <li>■ IP forwarding information</li> <li>■ BOOTP configuration</li> <li>■ VLAN name, VLANid</li> <li>■ Global ICMP configuration</li> <li>■ Global router advertisement configuration</li> </ul>
<code>show ip stats {vlan [&lt;name&gt;   all]}</code>	Displays IP statistics for the CPU of the Switch.
<code>show iparp {&lt;ipaddress&gt;   vlan &lt;name&gt;   all   permanent}</code>	Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, VLAN, or permanent entries. Each entry displayed includes the following: <ul style="list-style-type: none"> <li>■ IP address</li> <li>■ MAC address</li> <li>■ Aging timer value</li> <li>■ VLAN name, VLANid, and port number</li> <li>■ Flags</li> </ul>
<code>show ipfdb {&lt;ipaddress&gt; &lt;netmask&gt;   vlan &lt;name&gt;   all}</code>	Displays the contents of the IP forwarding database table. Used for technical support purposes.
<code>show iproute vlan {&lt;name&gt;   all   permanent   &lt;ipaddress&gt; &lt;netmask&gt;}</code>	Displays the contents of the IP routing table.
<code>show rip {vlan &lt;name&gt;   all}</code>	Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following: <ul style="list-style-type: none"> <li>■ Packets transmitted</li> <li>■ Packets received</li> <li>■ Bad packets received</li> <li>■ Bad routes received</li> <li>■ Number of RIP peers</li> <li>■ Peer information</li> </ul>

(continued)

**Table 8-5** Router Show Commands (continued)

Command	Description
<code>show rip stat {vlan &lt;name&gt;   all}</code>	Displays RIP-specific statistics. Statistics include the following per interface: <ul style="list-style-type: none"> <li>■ Packets transmitted</li> <li>■ Packets received</li> <li>■ Bad packets received</li> <li>■ Bad routes received</li> <li>■ Number of RIP peers</li> <li>■ Peer information</li> </ul>

## Resetting and Disabling Router Settings

To return router settings to their defaults and disable routing functions, use the commands listed in Table 8-6.

**Table 8-6** Router Reset and Disable Commands

Command	Description
<code>clear iparp [&lt;ipaddress&gt;   vlan &lt;name&gt;   all]</code>	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
<code>clear ipfdb [&lt;ipaddress&gt; &lt;netmask&gt;   vlan &lt;name&gt;   all]</code>	Removes the dynamic entries in the IP forwarding database.
<code>disable bootp vlan [&lt;name&gt;   all]</code>	Disables the generation and processing of BOOTP packets.
<code>disable bootprelay</code>	Disables the forwarding of BOOTP requests.
<code>disable icmp redirects {vlan &lt;name&gt;   all}</code>	Disables the generation of ICMP redirects on one or more VLANs.
<code>disable icmp unreachable</code>	Disables the generation of ICMP unreachable messages on one or more VLANs.
<code>disable icmp userredirects</code>	Disables the changing of routing table information when an ICMP redirect message is received.
<code>disable ipforwarding {vlan &lt;name&gt;   all}</code>	Disables routing for one or more VLANs.
<code>disable ipforwarding broadcast {vlan &lt;name&gt;   all}</code>	Disables routing of broadcasts to other networks.
<code>disable irdp {vlan &lt;name&gt;   all}</code>	Disables the generation of router advertisement messages on one or more VLANs.

(continued)

**Table 8-6** Router Reset and Disable Commands (continued)

Command	Description
<code>disable rip {vlan &lt;name&gt;   all}</code>	Disables RIP for one or more VLANs. When RIP is disabled, the parameters are not reset to their defaults, and the states are not cleared.  Disables RIP for a VLAN causes all routes learned from that VLAN to be advertised with a GarbageTime metric of 16, before being deleted from the route table.
<code>disable rip aggregation</code>	Disables the RIP aggregation of subnet information on a RIP version 2 interface.
<code>disable rip splithorizon</code>	Disables split horizon.
<code>disable rip poisonreverse</code>	Disables poison reverse.
<code>disable rip triggerupdate</code>	Disables triggered updates.
<code>disable rip exportstatic</code>	Disables the filtering of static routes.
<code>unconfig icmp</code>	Resets all ICMP settings to the default values.
<code>unconfig irdp</code>	Resets all router advertisement settings to the default values.
<code>unconfig rip {vlan &lt;name&gt;   all}</code>	Resets all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.

# 9

## STATUS MONITORING AND STATISTICS

This chapter describes how to view the current operating status of the Switch, how to display information in the Switch log, and how to take advantage of the RMON capabilities available in the Switch.

Viewing statistics on a regular basis allows you to:

- Monitor how well your network is performing
- Monitor emerging trends and notice problems arising before they cause major network faults

---

### Status Monitoring

The status monitoring facility provides information about the Switch. This information may be useful for your technical support representative if you have a problem.

Table 9-1 describes the monitoring commands available on the Switch.

**Table 9-1** Switch Monitoring Commands

Command	Description
<code>show account</code>	Displays the account names, access level, number of successful and failed logon attempts, and the number of active sessions in the user database. This command is available only to admin level users.
<code>show config</code>	Displays the current Switch configuration to the terminal. You can then capture the output and store it as a file.
<code>show fdb {all   &lt;macaddress&gt;   vlan &lt;name&gt;   &lt;portlist&gt;   permanent}</code>	Displays the forwarding database contents including MAC address, associated VLAN, port, age of entry configuration method, and status. Providing one of the options acts as a filter on the display. Providing a VLAN name displays all entries for the VLAN. Use the MAC address to locate a specific entry in the FDB.

(continued)

---

**Table 9-1** Switch Monitoring Commands (continued)

Command	Description
<code>show ip config {vlan &lt;name&gt;   all}</code>	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none"> <li>■ IP address, subnet mask</li> <li>■ IP forwarding information</li> <li>■ BOOTP configuration</li> <li>■ VLAN name, VLANid</li> </ul>
<code>show iparp {&lt;ip_address&gt;   vlan &lt;name&gt;   all   permanent}</code>	Displays the current Address Resolution Protocol (ARP) cache for a selected IP address, VLAN, or all entries. With no options, information for all VLANs is displayed. Information displayed includes IP address, MAC address, aging timer value, VLAN name, VLANid, and port number.
<code>show ipfdb {&lt;ipaddress&gt;   vlan &lt;name&gt;   all}</code>	Displays the contents of the IP forwarding database table. Use for technical support purposes.
<code>show iproute vlan {&lt;name&gt;   all   permanent}</code>	Displays the contents of the IP routing table.
<code>show ipstats {vlan [&lt;name&gt;   all]}</code>	Displays statistics of packets handled by the CPU, including the following: <ul style="list-style-type: none"> <li>■ inpackets, outpackets</li> <li>■ ICMP/IGMP statistics</li> <li>■ IRDP statistics</li> </ul>
<code>show log {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	Displays the current snapshot of the log. Options include: <ul style="list-style-type: none"> <li>■ <code>priority</code> — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.</li> </ul>
<code>show log config</code>	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
<code>show management</code>	Displays network management configuration and statics including enable/disable states for Telnet and SNMP, SNMP community strings, authorized SNMP station list, SNMP trap receiver list, and logon statistics.
<code>show memory</code>	Displays summary system configuration and memory utilization statistics for the CPU system DRAM.

(continued)

**Table 9-1** Switch Monitoring Commands (continued)

Command	Description
<code>show port &lt;portlist&gt; collisions</code>	Displays collision statistics for each port.
<code>show port &lt;portlist&gt; config</code>	Displays state, link status, speed, and autonegotiation setting for each port.
<code>show port &lt;portlist&gt; errors</code>	Displays error information for one or more ports.
<code>show port &lt;portlist&gt; packet</code>	Displays a histogram of packet statistics for one or more ports.
<code>show port &lt;portlist&gt; stats</code>	Displays port information including physical layer configuration and statistics.
<code>show port &lt;portlist&gt; util</code>	Displays port utilization by percentage, bytes per second, and packets per second. Use the space bar to toggle between percentage, bytes per second, and packets per second. Use the clear counters command to reset values.
<code>show protocol {&lt;protocol&gt;   all}</code>	Displays protocol information including protocol name, protocol fields, and the list of VLANs that use this protocol.
<code>show rip {vlan &lt;name&gt;   all}</code>	Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following: <ul style="list-style-type: none"> <li>■ Packets transmitted</li> <li>■ Packets received</li> <li>■ Bad packets received</li> <li>■ Bad routes received</li> <li>■ Number of RIP peers</li> <li>■ Peer information</li> </ul>
<code>show rip stat {vlan &lt;name&gt;   all}</code>	Displays RIP-specific statistics. Statistics include the following per interface: <ul style="list-style-type: none"> <li>■ Packets transmitted</li> <li>■ Packets received</li> <li>■ Bad packets received</li> <li>■ Bad routes received</li> <li>■ Number of RIP peers</li> <li>■ Peer information</li> </ul>
<code>show session</code>	Displays the currently active Telnet and console sessions communicating with the Switch. Provides the user name, IP address of the incoming Telnet session, whether a console session is currently active, and logon time. Sessions are numbered.
<code>show stpd {&lt;stpd_name&gt;   all}</code>	Displays STP information for one or all STP domains.

(continued)

**Table 9-1** Switch Monitoring Commands (continued)

Command	Description
<code>show stpd &lt;stpd_name&gt; port &lt;portlist&gt;</code>	Displays port-specific STP information, including STP port configuration and state.
<code>show switch</code>	Displays the current Switch information, including: <ul style="list-style-type: none"> <li>■ sysName, sysLocation, sysContact</li> <li>■ MAC address</li> <li>■ current time and date, and system uptime</li> <li>■ operating environment (temperature, fans, and power supply status)</li> <li>■ NVRAM image information (primary/secondary image, date, time, size, version)</li> <li>■ NVRAM configuration information (primary/secondary configuration, date, time, size, version)</li> <li>■ Scheduled reboot information</li> <li>■ 802.1p and PACE configuration information</li> <li>■ System serial number and hardware rework indicators</li> <li>■ Software platform</li> <li>■ System identifier</li> </ul>
<code>show version</code>	Displays the current running software image and configuration version number.
<code>show vlan {&lt;name&gt;   all}</code>	When used with the keyword <code>all</code> , or with no named VLANs, displays a summary list of VLAN names with a portlist and associated status of each. When used with a named identifier, displays port information including membership list, IP address, tag information.

## Port Statistics

The Switch 9000 provides a facility for viewing port statistic information. The summary information lists values for the current counter against every port on the Switch and it is refreshed approximately every 2 seconds. Values are displayed to 9 digits of accuracy.

To view port statistics, enter:

```
show port <portlist> stats
```



The following port statistic information is collected by the Switch:

**Link Status** — The current status of the link. Options are:

- Ready — The port is ready to accept a link.
- Active — The link is present at this port.

**Transmit Packet Count (Tx Pkt Count)** — The number of packets that have been successfully transmitted by the port.

**Transmit Byte Count (Tx Byte Count)** — The total number of data bytes successfully transmitted by the port.

**Total Collisions** — The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions. This value will always be zero for a full-duplex device.

**Received Packet Count (Rx Pkt Count)** — The total number of good packets that have been received by the port.

**Received Byte Count (RX Byte Count)** — The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the *Frame Check Sequence (FCS)*, but excludes bytes in the preamble.

**Receive Broadcast (RX Bcast)** — The total number of frames received by the port that are addressed to a broadcast address.

**Receive Multicast (RX Mcast)** — The total number of frames received by the port that are addressed to a multicast address.

---

## Port Errors

The Switch 9000 keeps track of errors for each port.

To view port error, type

```
show port <portlist> errors
```

The following port error information is collected by the Switch:

**Link Status** — The current status of the link. Options are:

- Ready — The port is ready to accept a link.
- Active — The link is present at this port.

**Transmit Collisions (TX Coll)** — The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions. This value will always be zero for a full-duplex device

**Transmit Late Collisions (TX Late)** — The total number of collisions that have occurred after the port's transmit window has expired. This value will always be zero for a full-duplex device.

**Transmit Deferred Frames (TX Def)** — The total number of frames that were transmitted by the port after the first transmission attempt was deferred by other network traffic.

**Transmit Frames Lost (TX Lost)** — The total number of frames that were not completely transmitted by the port.

**Transmit Errored Frames (TX Err)** — The total number of frames that were not completely transmitted by the port due to network errors, such as late collisions or excessive collisions.

**Receive Bad CRC Frames (RX CRC)** — The total number of frames received by the port that were of the correct length, but contained a bad FCS value.

**Receive Oversize Frames (RX Over)** — The total number of good frames received by the port that were of longer than the supported maximum length of 1522 bytes.

**Receive Undersize Frames (RX Under)** — The total number of frames received by the port that were less than 64 bytes long.

**Receive Jabber Frames (RX Jab)** — The total number of frames received by the port that were of longer than the support maximum length and had a *Cyclic Redundancy Check (CRC)* error.

**Receive Alignment Errors (RX Align)** — The total number of frames received by the port that occurs if a frame has a CRC error and does not contain an integral number of octets.

**Receive Frames Lost (RX Lost)** — The total number of frames received by the port that were lost.

## Switch Logging

The Switch 9000 log tracks all configuration and fault information pertaining to the device. Each entry in the log contains the following information:

- **Timestamp** — The timestamp records the month and day of the event, along with the time (hours, minutes, and seconds) in the form HH:MM:SS. If the event was caused by a user, the user name is also provided.
- **Fault level** — Table 9-2 describes the three levels of importance that the Switch can assign to a fault.

**Table 9-2** Fault Levels Assigned by the Switch

Level	Description
Critical	A desired Switch function is inoperable. The Switch may need to be reset.
Warning	A noncritical error that may lead to a function failure.
Informational	Actions and events that are consistent with expected behavior.

- **Subsystem** — The facility refers to the specific functional area of the Switch to which the error refers. Table 9-3 describes the subsystems.

**Table 9-3** Fault Log Subsystems

Subsystem	Description
Syst	General system-related information. Examples include memory, power supply, security violations, fan failure, overheat condition, and configuration mode.
STP	STP information. Examples include an STP state change.

**Table 9-3** Fault Log Subsystems

Subsystem	Description
Brdg	Bridge-related functionality. Examples include low table space and queue overflow.
SNMP	SNMP information. Examples include community string violations.
Telnet	Information related to Telnet logon and configuration performed by way of a Telnet session.
VLAN	VLAN-related configuration information.
Port	Port management-related configuration. Examples include port statistics and errors.

- **Message** — The message contains the log information with text that is specific to the problem.

### Local Logging

The Switch maintains 1,000 messages in its internal log. You can display a snapshot of the log at any given point in time by using the following command:

```
show log {<priority>} {<subsystem>}
```

where the following is true:

- **priority** — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.
- **subsystem** — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP, Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.

### Real-time Display

In addition to viewing a snapshot of the Switch log, you can configure the Switch to maintain a running real-time display of log messages on the console. To turn on the log display, use the following command:

```
enable log display
```

To configure the log display, use the following command:

```
config log display {<priority>} {<subsystem>}
```

If priority is not specified, only messages of critical priority are displayed. If the subsystem is not specified, all subsystems are displayed.

If you enable the log display on a terminal connected to the console port, your settings will remain in effect even after your console session is ended (unless you explicitly disable the log display).

When using a Telnet connection, if your Telnet session is disconnected (due to the inactivity timer, or for other reasons), the log display is automatically halted. You must restart the log display by using the `enable log display` command.

## Remote Logging

In addition to maintaining an internal log, the Switch 9000 supports remote logging by way of the UNIX Syslog host facility. To enable remote logging, do the following:

- Configure the Syslog host to accept and log messages.
- Enable remote logging by using the following command:

```
enable syslog
```

- Configure remote logging by using the following command:

```
config syslog <ipaddress> <facility> {<priority>}  
{<subsystem>}
```

Specify:

- **ipaddress** — The IP address of the syslog host.
- **facility** — The syslog facility level for local use. Options include `local0` through `local7`.
- **priority** — Filters the log to display message with the selected priority or higher (more critical). Priorities include `critical`, `warning`, and `informational`. If not specified, only critical priority messages are sent to the syslog host.
- **subsystem** — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include `Syst`, `STP`, `Brdg`, `SNMP`, `Telnet`, `VLAN`, and `Port`. If not specified, all subsystems are sent to the syslog host.



*Refer to your UNIX documentation for more information about the Syslog host facility.*

**Logging Commands** The commands described in Table 9-4 allow you to do the following:

- Configure logging options
- Reset logging options
- Display the log
- Clear the log

**Table 9-4** Logging Commands

Command	Description
<code>config log display {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	Allows you to configure the real-time log display. Options include: <ul style="list-style-type: none"> <li>■ <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP, Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.</li> </ul>
<code>config syslog &lt;ip_address&gt; &lt;facility&gt; {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	Allows you to configure the syslog host address and filter messages sent to the syslog host. Options include: <ul style="list-style-type: none"> <li>■ <code>ipaddress</code> — The IP address of the syslog host.</li> <li>■ <code>facility</code> — The syslog facility level for local use.</li> <li>■ <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, only critical priority messages and are sent to the syslog host.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP, Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are sent to the syslog host.</li> </ul>
<code>enable log display</code>	Allows you to enable the log display.
<code>enable syslog</code>	Allows you to enable logging to a remote syslog host.
<code>disable log display</code>	Allows you to disable the log display.
<code>disable syslog</code>	Allows you to disable logging to a remote syslog host.

(continued)

**Table 9-4** Logging Commands (continued)

Command	Description
<code>show log {&lt;priority&gt;} {&lt;subsystem&gt;}</code>	Allows you to display the a snapshot of the log. Options include: <ul style="list-style-type: none"> <li>■ <code>priority</code> — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.</li> <li>■ <code>subsystem</code> — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP, Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.</li> </ul>
<code>show log config</code>	Allows you to display the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
<code>clear counters</code>	Allows you to clear all statistical counters for the Switch and ports.
<code>clear log</code>	Allows you to clear the log.

**RMON**

Using the Remote Monitoring (RMON) capabilities of the Switch allows network administrators to make decisions about improving Switch efficiency and reducing the load on the network.

The following sections explain more about the RMON concept and the RMON features supported by the Switch 9000.



*You can only use the RMON features of the Switch if you have an RMON management application, such as the RMON application supplied with 3Com's Transcend® Enterprise Manager.*

**About RMON**

RMON is the common abbreviation for the Remote Monitoring Management Information Base (MIB) system defined by the Internet Engineering Task Force (IETF) documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of the following two components:

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

### About the RMON Groups

The Switch 9000 supports the following four RMON groups:

- Statistics
- History
- Alarms
- Events

This section describes how to use each of these groups to monitor your network.

#### Statistics

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

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

#### History

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

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



## Alarms

The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any MIB variable. Alarms inform you of a network performance problem and they can trigger automated action responses through the Events group.

## Events

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

## Benefits of RMON

Using the RMON features of your Switch has the following three main advantages:

- It improves network monitoring efficiency.
- It allows you to manage the network in a more proactive manner.
- It reduces the load on the network and the management workstation.

## Improving Efficiency

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

## Allowing Proactive Management

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

## Reducing the Traffic Load

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

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

### **RMON and the Switch**

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

For example, statistics can be related to individual ports and the Switch can take autonomous actions such as disabling a port (temporarily or permanently) if errors on that port exceed a predefined threshold. Also, since a probe must be able to see all traffic, a stand-alone probe must be attached to a nonsecure port. Implementing RMON in the Switch means that all ports can have security features enabled.

### **RMON Features of the Switch**

Table 9-5 details the RMON support provided by the Switch 9000.

**Table 9-5** RMON support supplied by the Switch 9000

<b>RMON Group</b>	<b>Support Supplied by the Switch</b>
<b>Statistics</b>	The Switch supports the EtherStats group.
<b>History</b>	A new or initialized Switch has two History sessions on each port: <ul style="list-style-type: none"> <li>■ 30-second intervals</li> <li>■ 2-hour intervals</li> </ul> The Switch can store a maximum of 50 History sessions.
<b>Alarms</b>	The Switch supports up to 50 alarms. You can enter or delete these alarms using an RMON management application.
<b>Events</b>	A new or initialized Switch has events defined for use with the default alarm system.

When using the RMON features of the Switch, you should note the following:

- After the default sessions are created, they have no special status. You can delete or change them as required.
- The greater the number of RMON sessions, the greater the burden on the management resources of the Switch. However, the forwarding performance of the Switch is not affected.

**About Event Actions**

You can define up to 50 alarms for the Switch. The actions that you can define for each alarm are shown in Table 9-6.

**Table 9-6** Event Actions

Action	High Threshold
No action	
Notify only	Send Trap.
Notify and log	Send trap. Place entry in RMON log.



# 10

## SOFTWARE UPGRADE AND BOOT OPTIONS

This chapter describes the procedure for upgrading the Switch software image. It also covers how to save and load a primary and secondary configuration file on the Switch.

---

### Upgrading the Software

The image file contains the executable code that runs on the Switch 9000. It comes preinstalled on the Switch from the factory. As new versions of the image are released, you should upgrade the software running on your Switch.

The image is upgraded by using a *Trivial File Transfer Protocol* (TFTP) server on the network. Downloading a new image involves the following:

- Load the new image onto a TFTP server on your network.
- Download the new image to the Switch 9000 using the following command:  

```
download image <ipaddress> <filename> {primary | secondary}
```

where:
  - **ipaddress** — is the IP address of the TFTP server
  - **filename** — is the filename of the new image
  - **primary | secondary** — (optional) indicates the image to which you want the file downloaded. If no parameter is specified, the file is saved to the primary image.

The Switch 9000 can store up to two images; a primary and a secondary. When you download a new image, you must select into which image space (primary or secondary) you want the new image to be placed.

You can select which image the Switch will load on the next reboot by using the following command:

```
use image {primary | secondary}
```

If you do not specify which image to use, the Switch automatically loads the primary image.

### Rebooting the Switch

To reboot the Switch, use the following command:

```
reboot
```

---

## Saving Configuration Changes

The configuration is the customized set of parameters that you have selected to run on the Switch. As you make configuration changes, the new settings are stored in run-time memory. Settings that are stored in run-time memory are not retained by the Switch when the Switch is rebooted. In order to retain the settings, and have them be loaded when you reboot the Switch, you must save the configuration to non-volatile storage.

The Switch 9000 can store two different configurations; a primary and a secondary. When you save configuration changes, you can select which configuration you want the changes saved to. If you do not specify, the changes are saved to the current configuration area.

If you have made a mistake, or have the need to go back to the configuration as it was before you started making changes, you can tell the Switch to use the unchanged configuration on the next reboot.

To save the configuration, use the following command:

```
save config {primary | secondary}
```

## Returning to Factory Defaults

To return the Switch configuration to factory defaults, use the following command:

```
unconfig switch
```

This command resets the entire configuration, with the exception of user accounts and passwords that have been configured.

To reset all parameters, use the following command:

```
unconfig switch all
```

---

## Boot Option Commands

Table 10-1 lists the commands associated with Switch 9000 boot options.

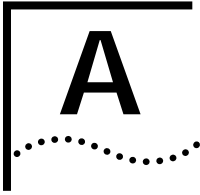
**Table 10-1** Boot Option Commands

Command	Description
<code>download image &lt;ipaddress&gt; &lt;filename&gt; {primary   secondary}</code>	Allows you to download a new image from a TFTP server. You must specify the IP address of the TFTP server and the image filename. You can optionally specify if you want the file downloaded to the primary or secondary image. If you do not specify, the file is downloaded to the primary image.
<code>save config {primary   secondary}</code>	Allows you to save the current configuration of the Switch to NVRAM. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the current configuration area in use.
<code>use config {primary   secondary}</code>	Allows you to configure the Switch to use a particular configuration on the next reboot. Options include the primary configuration area or the secondary configuration area.
<code>use image {primary   secondary}</code>	Allows you to configure the Switch to use a particular image on the next reboot. If not specified, the Switch will use the primary image.

---







# SAFETY INFORMATION

You must read the following safety information before carrying out any installation or removal of components, or any maintenance procedures on the Switch 9000.

---

## Important Safety Information



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

*Please read the following safety information thoroughly before installing the Switch 9000.*

- Installation and removal of the unit must be carried out by qualified personnel only.
- To reduce the risk of fire or electric shock, install the unit in a temperature and humidity controlled indoor area free of conductive contaminants.


### Power

- To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.
- Disconnect the power adapter before removing the unit.
- The unit must be earthed (grounded).
- The unit must be connected to an earthed (grounded) outlet to comply with European safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

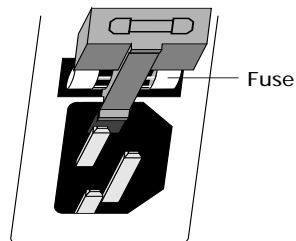
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN60320/IEC320 appliance inlet.
- *France and Peru only*  
This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground).  
†Impédance à la terre
- *United Kingdom only*  
The Switch 9000 is covered by Oftel General Approval, NS/G12345/J/100003, for indirect connection to a public telecommunications system. This can only be achieved using the console port on the unit and an approved modem.

### Power Cord

- This must be approved for the country where it is used:
  - USA and Canada
    - The cord set must be UL-approved and CSA certified.
    - The minimum specification for the flexible cord is:  
No. 18 AWG  
Type SV or SJ  
3-conductor
    - The cord set must have a rated current capacity of at least 10A.
    - The attachment plug must be an earth-grounding type with a NEMA 5-15P (15A, 125V) or NEMA 6-15P (15A, 250V) configuration.
  - Denmark
    - The supply plug must comply with section 107-2-D1, standard DK2-1a or DK2-5a.
  - Switzerland
    - The supply plug must comply with SEV/ASE 1011.

- If the power cord plug is unsuitable and must be replaced, you may find other codings for the respective connections. Connect the power supply wires for the unit according to the following scheme:
  - Brown wire to the Live (Line) plug terminal which may be marked with the letter 'L' or colored red.
  - Blue wire to the Neutral plug terminal which may be marked with the letter 'N' or colored black.
  - Yellow/Green wire to the Earth (Ground) plug terminal which may be marked with the letter 'E' or the Earth symbol  or colored yellow/green.

- Fuse**
- Disconnect power from the unit before opening the fuse holder cover. The unit automatically adjusts to the supply voltage. The fuse is suitable for both 110V A.C. and 220-240V A.C. operation. To change the fuse, release the fuse holder by gently levering a small screwdriver under the fuse holder catch. Only fuses of the same manufacturer, rating and type as the original must be used with the unit. Close the fuse holder.



- To comply with European safety standards, a spare fuse must not be fitted to the appliance inlet. Only fuses of the same manufacturer, make and type must be used with the unit.

### Fiber Optic Ports

- **Optical Safety.** Never look at the transmit LED/laser through a magnifying device while it is powered on. Never look directly at the fiber TX port and fiber cable ends when they are powered on.
- CLASS 1 LASER DEVICE

## Lithium Battery

- Replace the lithium battery with the same or equivalent type, as recommended by the manufacturer.



**WARNING:** There is a danger of explosion if the battery is incorrectly replaced.

- Dispose of used batteries according to the manufacturers instructions.
  - Do not disposed of the batteries in water, or by fire.
  - Disposal requirements vary by country and by state.
  - Lithium batteries are not an EPA listed hazardous waste. Therefore, they can typically be disposed of as normal waste.
  - If you are disposing of large quantities, contact a local waste management service.
- There are no hazardous compounds used within the battery module.
- The weight of the lithium contained in each coin cell is approximately 0.035 grams.
- Two types of batteries are used interchangeably:
  - CR chemistry uses manganese dioxide as the cathode material
  - BR chemistry uses poly-carbonmonofluoride as the cathode material.
- The battery in the bq4830 device is encapsulated and not user replaceable.

---

## L'information de Sécurité Importante



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

*Veillez lire à fond l'information de la sécurité suivante avant d'installer le Switch 9000.*

- L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.

- Pour réduire les risques d'incendie ou de choc électrique, installez ce groupe sous abri dans une zone dont la température et l'humidité sont régulées et qui ne contient pas de produits contaminateurs conductifs.
- Power**
- Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.
  - Débranchez l'adaptateur électrique avant de retirer cet appareil.
  - Vous devez mettre l'appareil à la terre (à la masse) ce groupe.
  - Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes européennes de sécurité.
  - Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).
  - La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.
  - L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.
  - Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN60320/CEI 320.
  - *France et Pérou uniquement*  
Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

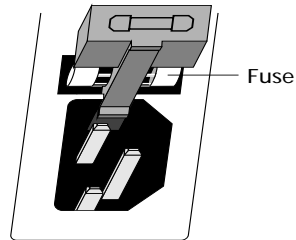
**Cordon électrique**

- Il doit être agréé dans le pays d'utilisation :
  - Etats-Unis et Canada
    - Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA
    - Le cordon souple doit respecter, à titre minimum, les spécifications suivantes :
      - calibre 18 AWG
      - type SV ou 5J
      - à 3 conducteurs
    - Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A
    - La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V)
  - Danemark
    - La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a
  - Suisse
    - La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011
- Si la prise mâle du cordon électrique est défectueuse, vous devez la remplacer en identifiant d'autres codages pour assurer les différentes connexions nécessaires. Branchez les fils d'alimentation électrique du groupe en respectant les principes suivants :
  - fil marron sur la borne de phase de la prise mâle, borne identifiée par la lettre "L" ou la couleur rouge
  - fil bleu sur la borne neutre de la prise femelle, borne identifiée par la lettre "N" ou la couleur noire
  - fil jaune/vert sur la borne de terre (masse) de la prise mâle, borne identifiée par la lettre "E", le symbole Mise à la terre ou la couleur jaune/verte

**Fuse**

- Mettez le groupe hors tension et avant d'ouvrir le couvercle porte-fusibles. Ce groupe se règle automatiquement sur la tension d'alimentation. Ce fusible convient à un fonctionnement sur une tension de 110 V c.a. ou de 220-240 V c.a.  
Pour changer ce fusible, libérez le porte-fusibles en plaçant doucement la lame d'un petit tournevis sous le cran de ce

porte-fusibles. Pour ce groupe, vous devez uniquement utiliser des fusibles réalisés par le même constructeur et offrant le même pouvoir de coupure et respectant le même type que le fusible d'origine. Refermez le porte-fusibles.



- Pour respecter les normes européennes de sécurité, il ne faut pas monter un fusible de rechange sur l'admission de cet appareil. Vous devez uniquement utiliser avec ce groupe des fusibles réalisés par le même constructeur, de même marque et de même type.

### Ports pour fibres optiques

- **Sécurité sur le plan optique.** Ne regardez jamais le voyant (DEL) d'émission/le laser en utilisant un dispositif d'agrandissement, tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.
- DISPOSITIF LASER DE CLASSE 1

### Batterie au lithium

- Remplacez la batterie au lithium par une batterie identique ou de type équivalent, en respectant les recommandations du constructeur.



**AVERTISSEMENT:** le remplacement incorrect de cette batterie présente un risque d'explosion.

- Vous devez vous débarrasser des batteries usées en respectant les consignes du fabricant :
  - ne jetez jamais ces batteries dans l'eau ou dans un feu.
  - les réglementations en matière d'élimination des batteries varient d'un pays à l'autre et d'un état à l'autre.

- les batteries au lithium ne figurent pas sur la liste EPA des déchets dangereux. Par conséquent, vous pouvez en général vous en débarrasser comme s'il s'agissait d'un déchet normal.
- si vous souhaitez vous débarrasser de quantités importantes, contactez un service local de gestion des déchets.
- Le module batteries ne contient aucun produit dangereux.
- Chaque cellule contient 0,035 gramme de lithium environ.
- Vous pouvez utiliser, de façon totalement libre, les deux types de batteries suivants :
  - la chimie CR utilise du dioxyde de manganèse comme matériau cathodique
  - la chimie du BR utilise du poly-carbonmonofluorure comme matériau cathodique
- Les batteries du dispositif bq4830 est hermétiquement scellé et ne peut donc pas être remplacé par l'utilisateur.

---

## Wichtige Sicherheitsinformat ionen



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

*Bitte unbedingt vor dem Einbauen des Switch 9000 Einheit die folgenden Sicherheitsanweisungen durchlesen.*

- Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.
- Um Brandgefahr oder Stromschläge auszuschließen, muß das Gerät in einem temperatur- und feuchtigkeitskontrollierten Innenraum aufgestellt werden, der frei von leitfähigen Schmutzstoffen ist.

### Power

- Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.
- Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.
- Das Gerät muß geerdet sein.



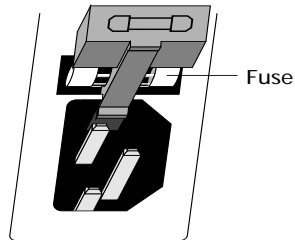
- Das Gerät muß an eine geerdete Steckdose angeschlossen werden, die die europäischen Sicherheitsnormen erfüllt.
- Das Gerät nicht an eine Wechselstromsteckdose anschließen, die nicht geerdet ist.
- Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.
- Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.
- Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß eine passende Konfiguration für einen Geräteeingang gemäß EN60320/IEC320 haben.

**Power Cord**

- Ist der Netzkabelstecker ungeeignet und muß ersetzt werden, so kann es sein, daß der andere Stecker unterschiedlich für die jeweiligen Anschlüsse kodiert ist. Die Netzkabeldrähte für das Gerät sind anhand des folgenden Schemas anzuschließen:
  - Braunen Draht an spannungsführende Leitungsklemme anschließen, die mit dem Buchstaben 'L' oder rot gekennzeichnet sein kann.
  - Blauen Draht an Neutralleiterklemme anschließen, die mit dem Buchstaben 'N' oder schwarz gekennzeichnet sein kann.
  - Gelb-grünen Draht an Masseleiterklemme anschließen, die mit dem Buchstaben 'E' oder dem Massesymbol oder gelb-grün gekennzeichnet sein kann.

**Fuse**

- Vor dem Öffnen der Sicherungsfassungsabdeckung den Netzstecker des Geräts abziehen. Das Gerät paßt sich automatisch an die Spannungsversorgung an. Die Sicherung ist für den Betrieb bei 110 Volt und 220 - 240 Volt (Wechselstrom) geeignet. Zum Auswechseln der Sicherung die Sicherungsfassung lösen. Dazu vorsichtig einen kleinen Schraubenzieher unter den Riegel der Fassung einführen. Es dürfen nur Sicherungen mit der gleichen Herstellernennspannung und vom gleichen Typ wie das Originalteil mit dem Gerät verwendet werden. Die Sicherungsfassung wieder schließen.



- Zur Erfüllung europäischer Sicherheitsnormen darf keine Ersatzsicherung am Geräteeingang angebracht werden. Es dürfen nur Sicherungen vom gleichen Hersteller, der gleichen Marke und Art mit dem Gerät verwendet werden.

### Faseroptikanschlüsse - Optische Sicherheit

- Niemals mit einem Vergrößerungsgerät ein Übertragungs-LED/Laser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.
- LASERGERÄT DER KLASSE 1

## Lithiumbatterie

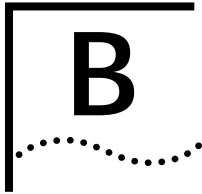
- Die Lithiumbatterie nach den Empfehlungen des Herstellers durch eine Batterie des gleichen oder eines gleichwertigen Typs ersetzen.



**WARNHINWEIS:** Wird die Batterie falsch ersetzt, besteht Explosionsgefahr.

- Verbrauchte Batterien nach den Angaben des Herstellers entsorgen.
  - Batterien nicht in Wasser eintauchen oder verbrennen.
  - Die Entsorgungsbestimmungen sind je nach Land verschieden.
  - Lithiumbatterien sind kein von der EPA aufgelisteter Sondermüll und können daher in der Regel mit dem normalen Müll entsorgt werden.
  - Bei der Entsorgung größerer Mengen ist die örtliche Müllverwaltungsstelle zu Rate zu ziehen.
- Das Batteriemodul enthält keine gefährlichen Verbindungen.
- In jeder Zelle ist ca. 0,035 g Lithium enthalten.
- Es werden zwei austauschbare Batterietypen verwendet.
  - CR-Chemie verwendet Mangandioxid als Kathodenmaterial.
  - BR-Chemie verwendet Poly-Kohlenstoffmonofluorid als Kathodenmaterial.
- Die Batterie im bq4830-Gerät ist eingekapselt und kann nicht vom Benutzer ersetzt werden.





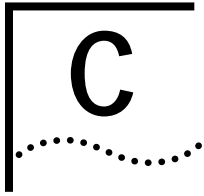
# TECHNICAL SPECIFICATIONS

<b>Physical Dimensions</b>	Height: 3.5 inches x Width: 17.32 inches x Depth: 17.32 inches Weight: 22 pounds
<b>Environmental Requirements</b>	
Operating Temperature	0 to 40° C
Storage Temperature	-10 to 70° C
Operating Humidity	10% to 95% relative humidity, noncondensing
Standards	EN60068 (IEC68)
<b>Safety</b>	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950, ECMA 97, EN60825-1
AC Protection	4A Fast Blow Fuse
<b>Electromagnetic Compatibility</b>	EN55022 Class B, FCC Part 15 Class A, ICES-003 Class A, VCCI Class 2, EN50082-1, ASIN23548 Class B
<b>Heat Dissipation</b>	118W maximum (341.2 BTU/hr maximum)
<b>Power Supply</b>	
AC Line Frequency	47Hz to 63Hz
Input Voltage Options	90VAC to 264VAC, auto-ranging
Current Rating	3A (maximum) at 100 VAC / 2A (maximum) at 240 VAC

---

<b>Standards Supported</b>	<b>SNMP</b>	<b>Protocols Used for Administration</b>
	SNMP protocol (RFC 1157)	UDP (RFC 768)
	MIB-II (RFC 1213)	IP (RFC 791)
	Bridge MIB (RFC 1493)	ICMP (RFC 792)
	VLAN MIB (RFC 1573)	TCP (RFC 793)
	RMON MIB (RFC 1757)	ARP (RFC 826)
	<b>Terminal Emulation</b>	TFTP (RFC 783)
	Telnet (RFC 854)	BOOTP (RFC 1271)

---



# TROUBLESHOOTING

If you encounter problems when using the Switch, this Appendix may be helpful. If you have a problem which is not listed here or in the release notes, please contact your local technical support representative.

---

## LEDs

### **Power LED does not light:**

Check that the power cable is firmly connected to the device and to the supply outlet.

Check the unit fuse. For information on changing the fuse, see Appendix A.

### **On powering-up, the MGMT LED lights yellow:**

The device has failed its Power On Self Test (POST) and you should contact your supplier for advice.

### **A link is connected, but the Status LED does not light:**

Check that:

- All connections are secure
- Cables are free from damage
- The devices at both ends of the link are powered-up
- Both ends of the gigabit link are set to the same auto-negotiation state

Both sides if the gigabit link must be enabled or disabled. If the two are different, typically the side with auto-negotiation disabled will have the link LED list, and the side with auto-negotiation enabled will not list. The default configuration for a gigabit port is auto-negotiation enabled. This can be verified by using the following command:

```
show port config
```

---

## Using the Command-Line Interface

### **The initial welcome prompt does not display:**

Check that your terminal or terminal emulator is correctly configured.

For console port access, you may need to press [Return] several times before the welcome prompt appears.

Check the settings on your terminal or terminal emulator. The settings are 9600 baud, 8 data bits, 1 stop bit, no parity, XON/OFF flow control enabled.

### **The SNMP Network Manager cannot access the device:**

Check that the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset.

Check that the device's IP address is correctly recorded by the SNMP Network Manager (refer to the user documentation for the Network Manager).

Check that the community strings configured for the Switch and network manager are the same.

Check that SNMP access was not disabled for the Switch.

### **The Telnet workstation cannot access the device:**

Check that the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address of the Switch correctly when invoking the Telnet facility. Check that Telnet access was not disabled for the Switch. If you attempt to logon and the maximum number of Telnet sessions are being used, you should receive an error message indicating so.



**Traps are not received by the SNMP Network Manager:**

Check that the SNMP Network Manager's IP address and community string are correctly configured and that the IP address of the Trap Receiver is configured properly on the Switch.

**The SNMP Network Manager or Telnet workstation can no longer access the device:**

Check that Telnet access or SNMP access is enabled.

Check that the port through which you are trying to access the device has not been disabled. If it is enabled, check the connections and network cabling at the port.

Check that the port through which you are trying to access the device is in a correctly configured VLAN.

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

There may be a network problem preventing you accessing the device over the network. Try accessing the device through the console port.

Check that the community strings configured for the Switch and the network manager are the same.

Check that SNMP access was not disabled for the Switch.

**Permanent entries remain in the FDB**

If you have made a permanent entry in the FDB, which requires you to specify the VLAN to which it belongs and then delete the VLAN, the FDB entry will remain. Though causing no harm, you must manually delete the entry from the FDB if you wish to remove it.

**Default and Static Routes**

If you have defined static or default routes, those routes will remain in the configuration independent of whether the VLAN and VLAN IP address that used them remains. You should manually delete the routes if no VLAN IP address is capable of using them.

### **You forget your password and cannot log on:**

If you are not an administrator, another user having administrator access level can log on, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having administrator access level can log in and initialize the device. This will return all configuration information, including passwords, to the initial values.

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

### **VLANs You cannot add a port to a VLAN:**

If you attempt to add a port to a VLAN and get an error message similar to the following:

```
localhost:7 # config vlan marketing add port 1,2
ERROR: Protocol conflict.
```

You already have a VLAN using untagged traffic on a port. Only one VLAN using untagged traffic can be configured on a single physical port. VLAN configuration can be verified by using the command

```
show vlan <name>
```

The solution for this error is to remove ports 1 and 2 from the VLAN currently using untagged traffic on those ports. If this was the 'default' VLAN, the command would be:

```
localhost:23 # config vlan default del port 1,2
```

which should now allow you to re-enter the previous command without error:

```
localhost:26 # config vlan red add port 1,2
```

## **VLAN Names:**

There are restrictions on VLAN names. They cannot contain white spaces and cannot start with a numeric value unless you use quotation marks around the name. If a name contains white spaces or starts with a numeric, you must use quotation marks whenever referring to the VLAN name.

## **802.1Q links do not work correctly:**

Remember that VLAN names are only locally significant through the command line interface. In order for two switches to communicate across a 802.1Q link, the VLANid for the VLAN on one switch should have a corresponding VLANid for the VLAN on the other switch.

If you are connecting to a third-party device and have checked that the VLANids are the same, the Ethertype field used to identify packets as 802.1Q packets may differ between the devices. The default value used by the switch is **8100**. If the third party device differs from this and cannot be changed, you may change the 802.1Q Ethertype used by the switch with the command:

```
config dot1p ethertype <ethertype>
```

Changing this parameter will change how the switch recognizes all tagged frames received and the value it inserts in all tagged frames it transmits.

## **VLANs, IP Addresses and default routes:**

Recall that the switch can have an IP address for each configured VLAN. It is only necessary to have an IP address associated with a VLAN if you intend to manage (telnet, SNMP, ping) through that VLAN. You can also configure multiple default routes for the switch. The switch will try first, the default route with the lowest cost metric.

## **STP You have connected an endstation directly to the Switch and the endstation fails to boot correctly:**

The Switch has STP enabled, and the endstation is booting before the STP initialization process is complete. Specify STP has been disabled, and then reboot the endstation.

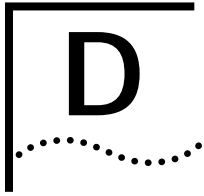
**The Switch keeps aging out endstation entries in the Switch Forwarding Database (FDB):**

Reduce the number of topology changes by disabling STP on those Switches that do not use redundant paths.

Specify that the endstation entries are static or permanent.

**Routing    The Switch sees RIP updates but other routers don't:**

Ensure that the RIP transmit and receive modes are appropriate for the environment. If other routers only use RIP Version 1, ensure the switch is transmitting V1 updates.



# TECHNICAL SUPPORT

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

Information contained in this appendix is correct at time of publication. For the very latest, we recommend that you access 3Com Corporation's World Wide Web site as described below.

---

## **Online Technical Services**

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

- World Wide Web site
- 3Com Bulletin Board Service (3ComBBS)
- 3ComFacts<sup>SM</sup> automated fax service
- 3ComForum on CompuServe<sup>®</sup> online service

## **World Wide Web Site**

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

**<http://www.3Com.com/>**

This service features news and information about 3Com products, customer service and support, 3Com Corporation's latest news releases, *NetAge* Magazine, and more.

## **3Com Bulletin Board Service**

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem or ISDN 24 hours a day, 7 days a week.

### **Access by Analog Modem**

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

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	61 2 9955 2073
Brazil	up to 14400 bps	55 11 547 9666
France	up to 14400 bps	33 1 6986 6954
Germany	up to 28800 bps	4989 62732 188
Hong Kong	up to 14400 bps	852 2537 5608
Italy (fee required)	up to 14400 bps	39 2 27300680
Japan	up to 14400 bps	81 3 3345 7266
Mexico	up to 28800 bps	52 5 520 7853
P. R. of China	up to 14400 bps	86 10 684 92351
Singapore	up to 14400 bps	65 534 5693
Taiwan	up to 14400 bps	886 2 377 5840
U.K.	up to 28800 bps	44 1442 438278
U.S.A.	up to 28800 bps	1 408 980 8204

### Access by Digital Modem

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

**408 654 2703**

### 3ComFacts<sup>SM</sup> Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone using one of these international access numbers:

Country	Telephone Number
Hong Kong	852 2537 5610
U.K.	44 1442 278279
U.S.A.	1 408 727 7021

Local access numbers are available within the following countries:

Country	Telephone Number	Country	Telephone Number
Australia	1 800 123853	Netherlands	06 0228049
Belgium	0800 71279	Norway	800 11062
Denmark	800 17319	Portugal	0505 442 607
Finland	98 001 4444	Russia (Moscow only)	956 0815
France	05 90 81 58	Spain	900 964 445
Germany	0130 81 80 63	Sweden	020 792954
Italy	1678 99085	U.K.	0800 626403

### 3ComForum on CompuServe® Online Service

3ComForum is a CompuServe-based service containing patches, software, drivers, and technical articles about all 3Com products, as well as a messaging section for peer support. To use 3ComForum, you need a CompuServe account.

To use 3ComForum:

- 1 Log on to CompuServe.
- 2 Type **go threecom**
- 3 Press [Return] to see the 3ComForum main menu.

### Support from Your Network Supplier

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

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

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

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

**Support from 3Com**

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

Contact your local 3Com sales office to find your authorized service provider using one of these numbers:

Regional Sales Office	Telephone Number	Regional Sales Office	Telephone Number
<b>3Com Corporation</b>		<b>3Com Ireland</b>	353 1 820 7077
U.S.	800 NET 3Com <i>or</i> 1 408 764 5000	<b>3Com Japan</b>	81 3 3345 7251
<b>3Com ANZA</b>		<b>3Com Latin America</b>	
East	61 2 9937 5000	Argentina	54 1 312 3266
West	61 3 9866 8022	Brazil	55 11 546 0869
<b>3Com Asia Limited</b>		Chile	56 2 633 9242
China	86 10 68492 568 (Beijing) 86 21 6374 0220 Ext 6115 (Shanghai)	Colombia	57 1 629 4110
Hong Kong	852 2501 1111	Mexico	52 5 520 7841
India	91 11 644 3974	Peru	51 1 221 5399
Indonesia	62 21 523 9181	Venezuela	58 2 953 8122
Korea	82 2 319 4711	<b>3Com Mediterraneo</b>	
Malaysia	60 3 732 7910	Italy	39 2 253011 (Milan) 39 6 5279941 (Rome)
Singapore	65 538 9368	<b>3Com Middle East</b>	971 4 349049
Taiwan	886 2 377 5850	<b>3Com Nordic AB</b>	
Thailand	662 231 8151 4	Denmark	45 39 27 85 00
<b>3Com Benelux B.V.</b>		Finland	358 0 435 420 67
Belgium	32 725 0202	Norway	47 22 18 40 03
Netherlands	31 30 6029700	Sweden	46 8 632 56 00
<b>3Com Canada</b>		<b>3Com Russia</b>	007 095 2580940
Calgary	403 265 3266	<b>3Com South Africa</b>	27 11 807 4397
Montreal	514 683 3266	<b>3Com UK Limited</b>	
Ottawa	613 566 7055		44 131 2478558 (Edinburgh)
Toronto	416 498 3266		44 161 8737717 (Manchester)
Vancouver	604 434 3266		44 1628 897000 (Marlow)
<b>3Com France</b>	33 1 69 86 68 00		
<b>3Com GmbH</b>			
Austria	43 1 5134323		
Czech and Slovak Republics	42 2 21845 800		
Germany	49 30 3498790 (Berlin) 49 89 627320 (Munich)		
Hungary	36 1 250 83 41		
Poland	48 22 6451351		
Switzerland	41 31 996 14 14		



---

**Returning Products  
for Repair**

Before you send a product directly to 3Com for repair, you must first be obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

<b>Country</b>	<b>Telephone Number</b>	<b>Fax Number</b>
U.S.A. and Canada	1 800 876 3266, option 2	408 764 7120
Latin America	1 408 326 7801	408 764 7120
Europe, South Africa and Middle East	44 1442 438125	44 1442 435822
Outside Europe, U.S.A., and Canada	1 408 326 7804	1 408 764 7120



# GLOSSARY

- ageing** The automatic removal of dynamic entries from the Switch Database that have timed-out and are no longer valid.
- ARP** Address Resolution Protocol. The protocol used to dynamically bind high-level IP addresses to low-level hardware addresses. ARP is used only across a single physical network and is limited to networks that support hardware broadcasts.
- backbone** The part of a network used as the primary path for transporting traffic between network segments.
- bandwidth** Information capacity, measured in bits per second (bps), that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps, the bandwidth of Gigabit Ethernet is 1000 Mbps.
- baud rate** The switching speed of a serial line. Also known as *line speed*.
- BOOTP** A protocol that allows automatic mapping of an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.
- bridge** A device that interconnects local or remote networks no matter what higher-level protocols are involved. Bridges form a single logical network.
- broadcast** A message sent to all destination devices on the network.
- broadcast storm** Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.
- console port** The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

**CSMA/CD** Carrier Sense Multiple Access/Collision Detection that is a channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

**data center switching** The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

**Ethernet** A LAN specification developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks operate at 10 Mbps using *CSMA/CD* to run over cabling.

**Fast Ethernet** 100 Mbps technology based on the Ethernet/CD network access method.

**forwarding** The process of sending a frame toward its destination by an internetworking device.

**full duplex** A system that allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a link.

**Gigabit Ethernet** 1000 Mbps technology based on the Ethernet/CD network access method, IEEE 802.3Z.

**ICMP** Internet Control Message Protocol. An integral part of the Internet Protocol (IP) that handles error and control messages. Gateways and hosts use ICMP to report problems about datagrams back to the original source that sent the datagram. ICMP also includes an echo require/reply used to test whether a destination is reachable and responding.

**IETF** Internet Engineering Task Force. A group of people concerned with short- and medium-term problems with TCP/IP and the connected Internet.

**IP address** Internet Protocol address that is a unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section, and a host section.

<b>LAN</b>	Local Area Network that consists of connected computing resources (such as PCs, printers, and servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.
<b>latency</b>	The delay between the time a device receives a frame and the time the frame is forwarded out of the destination port.
<b>line speed</b>	See <i>baud rate</i> .
<b>MAC</b>	Media Access Control. A method for controlling access to a transmission medium. An example is the Ethernet CSMA/CD access method.
<b>MIB</b>	Management Information Base that stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.
<b>multicast</b>	Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.
<b>NVRAM</b>	Non-volatile RAM. NVRAM retains its contents when the Switch is powered off.
<b>PACE</b>	Priority Access Control Enabled that is 3Com's innovative technology to work in conjunction with a switch in order to control the latency and jitter associated with the transmission of multimedia traffic over Ethernet and Fast Ethernet.
<b>POST</b>	Power On Self Test that is an internal test the Switch carries out when it is started up.
<b>protocol</b>	A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing, and error control.
<b>RMON</b>	Remote Monitoring that is a subset of SNMP MIB II and that allows monitoring and management capabilities by addressing up to 10 different groups of information.
<b>server farm</b>	A cluster of servers in a centralized location serving a wide user population.
<b>SNMP</b>	Simple Network Management Protocol that was originally designed to be used in managing TCP/IP internets. SNMP is presently implemented

on a wide range of computers and networking equipment and may be used to manage many aspects of network and endstation operation.

**Spanning Tree Protocol (STP)**

A bridge-based mechanism for providing fault tolerance on networks. STP works by allowing the implementation of parallel paths for network traffic, and ensuring that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

**switch**

A device that filters, forwards, and floods frames based on the frame's destination address. The Switch learns the addresses associated with each Switch port and builds tables based on this information to be used for the switching decision.

**TCP/IP**

A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

**Telnet**

A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

**TFTP**

Trivial File Transfer Protocol that allows the transfer of files (such as software upgrades) from a remote device using the Switch's local management capabilities.

**Transcend**

3Com's umbrella management system used to manage all of 3Com's networking solutions.

**trap**

A message sent by an SNMP agent to an authorized trap receiver (usually a network management station) to indicate the occurrence of a significant event, such as an error condition or a threshold that has been reached.

**UDP**

User Datagram Protocol that is an Internet standard protocol allowing an application program on one device to send a datagram to an application program on another device.

**VLAN**

Virtual LAN that is a group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

# INDEX

---

## Numerics

3Com Bulletin Board Service (3ComBBS) D-1  
3Com sales offices D-4  
3Com URL D-1  
3ComFacts D-2  
3ComForum D-3

---

## A

accounts, creating 3-3  
alarms 9-15  
Alarms (RMON group) 9-13, 9-14  
autonegotiation 3-13

---

## B

BOOTP 3-5  
Bridge Identifier 7-3  
bridge priority, configuring 4-14, 7-11  
bulletin board service D-1

---

## C

CompuServe D-3  
configuration changes, saving 10-2  
console port 1-8  
    connecting equipment to 2-4  
conventions  
    notice icons, About This Guide 3  
    text, About This Guide 3

---

## D

default  
    passwords 3-2  
    settings 1-9  
    users 3-2  
Default VLAN 5-11  
deleting a session 3-8  
device mode, configuring 8-4  
disconnecting a Telnet session 3-7  
dynamic entries 6-1  
dynamic routes 8-3

---

## E

EMC statement ii  
Events (RMON group) 9-13, 9-14

---

## F

fax service. *See* 3ComFacts  
FDB  
    configuring 6-3  
    creating a permanent entry 6-3  
    displaying 6-3  
    dynamic entries 6-1  
    entries 6-1  
    permanent entries 6-2  
    removing entries 6-4  
    static entries 6-1  
forward delay, configuring 4-14, 7-11  
Forwarding Database. *See* FDB  
free-standing installation 2-3  
full duplex 1-3

---

## G

Gigabit Ethernet  
    configuration rules 2-2  
    ports 1-2

---

## H

Hello Time  
    configuring 4-13, 7-11  
    description 7-4  
History (RMON group) 9-12, 9-14

---

## I

ICMP configuration commands (table) 8-9  
IEEE 802.1Q 5-6  
image, downloaded 10-1  
installing the switch 2-2  
IP address, entering 3-6  
IP unicast routing  
    configuration examples 8-10  
    configuring 8-4  
    default gateway 8-1  
    disabling 8-13  
    enabling 8-4  
    reset and disable commands (table) 8-13  
    resetting 8-13  
    router interfaces 8-1  
    router show commands (table) 8-12  
    routing table  
        configuration commands (table) 8-7

dynamic routes 8-3  
 populating 8-2  
 static routes 8-3  
 settings, displaying 8-12

---

## L

LEDs 1-7  
 load sharing 3-14  
 Load Sharing, configuring 3-15  
 log display 9-8  
 logging  
   and Telnet 9-9  
   commands 9-10  
   fault level 9-7  
   local 9-8  
   real-time display 9-8  
   remote 9-9  
   subsystem 9-7  
   timestamp 9-7  
 logging on 3-2

---

## M

Max Age, configuring 4-14, 7-11  
 media types, supported 2-2

---

## N

network supplier support D-3

---

## O

on-line technical services D-1

---

## P

passwords  
   default 3-2  
   forgetting 3-4  
 path costs  
   configuring 4-14, 7-11  
 permanent entries 6-2  
 port errors 9-6  
 port priority, configuring 4-14, 7-11  
 port statistics 9-4  
 power on self-test (POST) 2-6  
 power socket 1-8  
 power supply 1-8  
 Protocol Filter 5-9, 5-10  
 protocol filter 4-11, 5-8, 5-9

---

## R

rack mounting 2-2  
 rebooting 10-2  
 Remote Monitoring. *See* RMON  
 reset button 1-8  
 resetting to factory defaults 10-3  
 returning products for repair D-5  
 RIP  
   configuration commands (table) 8-7  
   enabling 8-4  
 RMON  
   alarm actions 9-15  
   features supported 9-14  
   groups supported 9-14  
   probe 9-12  
 Routing Information Protocol. *See* RIP  
 routing table, populating 8-2  
 routing. *See* IP unicast routing

---

## S

safety information  
   English A-1  
   French A-4  
   German A-8  
 serial number, location on the unit 1-8  
 serial port. *See* console port  
 sessions, deleting 3-8  
 SNMP, management 3-8  
 socket, power 1-8  
 software upgrade 10-1  
 Spanning Tree Protocol. *See* STP  
 standards supported B-2  
 static entries 6-1  
 static routes 8-3  
 statistics  
   port errors 9-6  
   port status 9-4  
 Statistics (RMON group) 9-12, 9-14  
 status monitoring 9-1  
 STP  
   Bridge Identifier 7-3  
   bridge priority 4-14, 7-11  
   commands 7-10  
   configuring 7-10  
   description 1-3  
   disabling and restoring defaults 7-14  
   displaying settings 7-12  
   domains 7-4  
   enabling 7-10  
   forward delay 4-14, 7-11  
   Hello Time  
     configuring 4-13, 7-11  
     description 7-4



- Max Age
  - configuring 4-14, 7-11
  - overview 7-1
  - path costs 4-14, 7-11
  - port priority 4-14, 7-11
- Switch 9000
  - configuration examples 1-4
  - dimensions B-1
  - factory defaults 1-9
  - features 1-1
  - free-standing installation 2-3
  - front view 1-6
  - Gigabit Ethernet ports 1-6
  - installing 2-2
  - LEDs 1-7
  - positioning 2-1
  - rack mounting 2-2
  - rear view 1-8
  - size B-1
  - stacking with other devices 2-4
  - weight B-1
- syslog host 9-9

- configuration examples 5-12
- configuring 5-11
- Default 5-11
- description 1-3, 5-1
- displaying settings 5-13
- names 5-10
- port-based 5-2
- restoring default values 5-15
- tagged 5-6
- types 5-2
- VLANid 5-6

---

## T

- technical support D-1
  - 3Com URL D-1
  - bulletin board service D-1
  - fax service D-2
  - network suppliers D-3
  - product repair D-5
  - using CompuServe D-3
- Telnet
  - disconnecting a session 3-7
  - using 3-5
- TFTP server 10-1
- trunk 5-6

---

## U

- upgrading software 10-1
- URL D-1
- users
  - creating 3-3
  - default 3-2
  - viewing 3-4

---

## V

- viewing accounts 3-4
- Virtual LANs. *See* VLANs
- VLAN tagging 5-6
- VLANid 5-6
- VLANs
  - benefits 5-1

---

## W

- World Wide Web D-1
- WWW D-1



# 3Com Corporation LIMITED WARRANTY

---

## HARDWARE

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

Network adapters	Lifetime
Other hardware products (unless otherwise specified above)	1 year
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

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

---

## SOFTWARE

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

---

## STANDARD WARRANTY SERVICE

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

---

## WARRANTIES EXCLUSIVE

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

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

---

**LIMITATION OF LIABILITY**

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation for personal injury, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

---

**GOVERNING LAW**

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

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

9/1/96