

User Manual for the NETGEAR 7200 Series Layer 2 Managed Switch Software



NETGEAR

NETGEAR, Inc.

4500 Great America
Parkway

Santa Clara, CA

202-10010-01
November 2003

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to <http://www.netgear.com>. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at: <http://www.netgear.com/> through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

Trademarks

NETGEAR is a registered trademark of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Regulatory Compliance Information

This device is restricted to indoor use due to reduce the potential for harmful interference to co-channel Mobile Satellite and Radar Systems.

Canadian Department of Communications Compliance Statement

This Class B Digital apparatus (GSM7224 Layer 2 Managed Switch) meets all the requirements of the Canadian Interference Causing Equipment Regulations.

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

This device complies with Class B limits of Industry of Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EN 55 022 Declaration of Conformance

This is to certify that the GSM7224 Layer 2 Managed Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Contents

- Chapter 1**
 - About This Guide**
 - Audience1-1
 - Why the Document was Created1-1
 - How to Use This Document1-1
 - Typographical Conventions1-2
 - Special Message Formats1-2
 - Features of the HTML Version of this Manual1-3
 - How to Print this Manual1-4
 - Chapter 2**
 - Switch Management Overview**
 - Scope2-1
 - Switch Management Overview2-1
 - Chapter 3**
 - Command Line Interface Syntax**
 - Format3-1
 - Command3-2
 - Parameters3-2
 - Values3-2
 - Conventions3-3
 - Annotations3-4
 - Chapter 4**
 - Administration Console Telnet Interface**
 - Set Up Your Switch Using Direct Console Access4-1
 - Chapter 5**
 - Web-Based Management Interface**
 - Web Based Management Overview5-1
 - How to Log In to the GSM72245-2
 - Web-Based Management Utility Features5-3
 - Interactive Switch Image5-3
 - Menus5-3

System-Wide Popup Menus	5-4
Port-Specific Popup Menus	5-4

Chapter 6

Quick Startup

Quick Starting the Switch	6-1
System Info and System Setup	6-2
Quick Startup Software Version Information	6-2
Quick Startup Physical Port Data	6-3
Quick Startup User Account Management	6-3
Quick Startup IP Address	6-4
Quick Startup Uploading from Switch to Out-of-Band PC (Only XMODEM)	6-6
Quick Startup Downloading from Out-of-Band PC to Switch (Only XMODEM)	6-6
Quick Startup Downloading from TFTP Server	6-7
Quick Startup Factory Defaults	6-7
VLAN Configuration Example	6-8
Solution 1	6-9
Solution 2	6-9

Chapter 7

Switching Commands

System Information and Statistics Commands	7-1
show inventory	7-1
show sysinfo	7-2
config sysname	7-2
config syslocation	7-3
config syscontact	7-3
show arp switch	7-3
show forwardingdb table	7-3
show forwardingdb learned	7-4
show stats port detailed	7-4
show stats port summary	7-9
show stats switch detailed	7-10
show stats switch summary	7-11
show eventlog	7-12
show msglog	7-12
show traplog	7-12

Management Commands	7-13
show network	7-13
config network macaddr	7-13
config network mactype	7-14
config network parms	7-14
config network protocol	7-14
config network webmode	7-14
config network javamode	7-15
config prompt	7-15
show serial	7-15
config serial baudrate	7-16
config serial timeout	7-16
show serviceport	7-16
config serviceport parms	7-16
config serviceport protocol	7-16
show snmpcommunity	7-17
config snmpcommunity accessmode	7-17
config snmpcommunity create	7-18
config snmpcommunity delete	7-18
config snmpcommunity ipaddr	7-18
config snmpcommunity ipmask	7-18
config snmpcommunity mode	7-19
show snmptrap	7-19
config snmptrap create	7-19
config snmptrap delete	7-19
config snmptrap ipaddr	7-20
config snmptrap mode	7-20
show trapflags	7-20
config trapflags authentication	7-21
config trapflags bcaststorm	7-21
config trapflags linkmode	7-21
config trapflags multiusers	7-21
config trapflags stpmode	7-21
show telnet	7-22
config telnet maxsessions	7-22

config telnet mode	7-22
config telnet timeout	7-22
show forwardingdb agetime	7-23
config forwardingdb agetime	7-23
Device Configuration Commands	7-23
show switchconfig	7-24
config switchconfig broadcast	7-24
config switchconfig flowcontrol	7-24
show port	7-24
config port adminmode	7-25
config port flowcontrol	7-25
config port linktrap	7-26
config port physicalmode	7-26
config port lacpmode	7-26
config port autoneg	7-26
show lag	7-26
config lag create	7-27
config lag addport	7-27
config lag deleteport	7-27
config lag adminmode	7-28
config lag linktrap	7-28
config lag name	7-28
config lag deletelag	7-28
config lag stpmode	7-28
show vlan summary	7-29
show vlan detailed	7-29
config vlan create	7-30
config vlan delete	7-30
config vlan name	7-30
config vlan makestatic	7-31
config vlan participation	7-31
config vlan port tagging	7-31
show vlan port	7-32
config vlan port pvid	7-32
config vlan port acceptframe	7-32

config vlan port ingressfilter	7-33
show protocol	7-33
config protocol create	7-33
config protocol delete	7-33
config protocol protocol add	7-34
config protocol protocol remove	7-34
config protocol vlan add	7-34
config protocol vlan remove	7-34
config protocol interface add	7-35
config protocol interface remove	7-35
show garp info	7-35
show garp interface	7-35
config garp gmrp adminmode	7-36
config garp gmrp interface mode	7-36
config garp gvrp adminmode	7-37
config garp gvrp interface mode	7-37
config garp jointimer	7-37
config garp leavetimer	7-37
config garp leavealltimer	7-38
show igmpsnooping	7-38
config igmpsnooping adminmode	7-39
config igmpsnooping groupmembershipinterval	7-39
config igmpsnooping maxresponse	7-39
config igmpsnooping mcrtrexpiretime	7-39
config igmpsnooping interface mode	7-40
show mfdb table	7-40
show mfdb gmrp	7-40
show mfdb igmpsnooping	7-41
show mfdb staticfiltering	7-41
show mfdb stats	7-42
show mirroring	7-42
config mirroring create	7-42
config mirroring delete	7-43
config mirroring mode	7-43
show macfilter	7-43

config macfilter create	7-43
config macfilter remove	7-44
config macfilter addsrc	7-44
config macfilter delsrc	7-44
config macfilter adddest	7-45
config macfilter deldest	7-45
Spanning Tree Commands	7-45
show spanningtree summary	7-46
config spanningtree adminmode	7-46
config spanningtree forceversion	7-47
config spanningtree configuration name	7-47
config spanningtree configuration revision	7-47
show spanningtree port	7-47
config spanningtree port migrationcheck	7-48
config spanningtree port mode	7-48
show spanningtree bridge	7-48
config spanningtree bridge maxage	7-49
config spanningtree bridge hellotime	7-49
config spanningtree bridge forwarddelay	7-49
config spanningtree bridge priority	7-49
show spanningtree cst detailed	7-49
show spanningtree cst port summary	7-50
show spanningtree cst port detailed	7-51
config spanningtree cst port pathcost	7-51
config spanningtree cst port priority	7-52
config spanningtree cst port edgeport	7-52
config spanningtree mst create	7-52
config spanningtree mst delete	7-52
config spanningtree mst vlan add	7-53
config spanningtree mst vlan remove	7-53
config spanningtree mst priority	7-53
config spanningtree mst port pathcost	7-53
config spanningtree mst port priority	7-54
show spanningtree mst summary	7-54
show spanningtree mst detailed	7-54

show spanningtree mst port summary	7-55
show spanningtree mst port detailed	7-55
show spanningtree vlan	7-55
User Account Management Commands	7-56
show users	7-56
config users add	7-56
config users passwd	7-57
config users delete	7-57
config users snmpv3 authentication	7-57
config users snmpv3 encryption	7-57
config users snmpv3 accessmode	7-58
show login session	7-58
config login session close	7-58
Security Commands	7-58
config radius maxretransmit	7-59
config radius timeout	7-59
config radius accounting mode	7-59
config radius accounting server add	7-60
config radius accounting server port	7-60
config radius accounting server remove	7-60
config radius accounting server secret	7-60
config radius server add	7-61
config radius server port	7-61
config radius server remove	7-61
config radius server secret	7-61
config radius server primary	7-62
config radius server msgauth	7-62
show radius summary	7-62
show radius server summary	7-62
show radius server stats	7-63
show radius accounting summary	7-64
show radius accounting stats	7-64
show radius stats	7-65
clear radius stats	7-65
config dot1x adminmode	7-65

config dot1x port initialize	7-65
config dot1x port reauthenticate	7-65
config dot1x port controldir	7-66
config dot1x port controlmode	7-66
config dot1x port quietperiod	7-66
config dot1x port transmitperiod	7-67
config dot1x port supptimeout	7-67
config dot1x port servertimeout	7-67
config dot1x port maxrequests	7-67
config dot1x port reauthperiod	7-67
config dot1x port reauthenabled	7-68
show dot1x summary	7-68
show dot1x port summary	7-68
show dot1x port detailed	7-68
show dot1x port stats	7-69
clear dot1x port stats	7-70
config authentication login create	7-70
config authentication login delete	7-71
config authentication login set	7-71
config dot1x defaultlogin	7-72
config dot1x login	7-72
config dot1x port users add	7-72
config dot1x port users remove	7-72
config users defaultlogin	7-72
config users login	7-73
show authentication login info	7-73
show authentication login users	7-73
show dot1x port users	7-73
show users authentication	7-74
System Utilities	7-74
save config	7-74
logout	7-74
transfer upload mode	7-74
transfer upload serverip	7-75
transfer upload path	7-75

transfer upload filename	7-76
transfer upload datatype	7-76
transfer upload start	7-76
transfer download mode	7-76
transfer download serverip	7-77
transfer download path	7-77
transfer download filename	7-77
transfer download datatype	7-77
transfer download start	7-78
clear transfer	7-78
clear config	7-78
clear pass	7-78
clear traplog	7-78
clear vlan	7-78
clear lag	7-79
clear stats port	7-79
clear stats switch	7-79
clear igmpsnooping	7-79
reset system	7-79
ping	7-80

Chapter 8

Differentiated Services

Appendix A

Cabling Guidelines

Fast Ethernet Cable Guidelines	9-1
Category 5 Cable	9-2
Category 5 Cable Specifications	9-2
Twisted Pair Cables	9-3
Patch Panels and Cables	9-4
Using 1000BASE-T Gigabit Ethernet over Category 5 Cable	9-5
Cabling	9-5
Near End Cross Talk (NEXT)	9-6
Patch Cables	9-6
RJ-45 Plug and RJ-45 Connectors	9-6
Conclusion	9-8

Appendix B
Glossary

Numeric	10-1
A	10-2
B	10-2
C	10-3
D	10-4
E	10-5
F	10-6
G	10-7
H	10-8
I	10-8
L	10-9
M	10-10
N	10-11
O	10-12
P	10-12
Q	10-13
R	10-13
S	10-14
T	10-16
U	10-17
V	10-17
W	10-17
X	10-18

Index

Chapter 1

About This Guide

Thank you for purchasing the NETGEAR™ GSM7224 L2 Switch.

Audience

This reference manual assumes that the reader has basic-to-intermediate computer and Internet skills. However, basic computer network, Internet, and wireless technology tutorial information is provided in the Appendices.

This document describes configuration commands for the GSM7224 Layer 2 Managed Switch software. The commands can be accessed from the CLI, telnet, and Web interfaces.

Why the Document was Created

This document was created primarily for system administrators configuring and operating a system using managed switch software. It is intended to provide an understanding of the configuration options of GSM7224 L2 Switch software.

It is assumed that the reader has an understanding of the relevant switch platforms. It is also assumed that the reader has a basic knowledge of Ethernet and networking concepts.

How to Use This Document

This document describes configuration commands for the GSM7224 Layer 2 Managed Switch software. The commands can be accessed from the CLI, telnet, and Web interfaces.

- [Chapter 6, “Quick Startup”](#) details the procedure to quickly become acquainted with the GSM7224 L2 Switch Software.
- [Chapter 7, “Switching Commands”](#) describes the Switching commands.

Note: Refer to the release notes for the GSM7224 Layer 2 Managed Switch Software application level code. The release notes detail the platform specific functionality of the Switching, SNMP, Config, and Management packages.

Typographical Conventions

This guide uses the following typographical conventions:

Table 1. Typographical conventions

<i>italics</i>	Emphasis.
bold times roman	User input.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
SMALL CAPS	DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
---	--

This manual is written for the GSM7224 L2 Switch according to these specifications:

Table 1-1. Manual Specifications

Product Version	GSM7224 Layer 2 Managed Switch
Manual Publication Date	November 2003

	Note: Product updates are available on the NETGEAR, Inc. Web site at http://www.netgear.com/support/main.asp . Documentation updates are available on the NETGEAR, Inc. Web site at http://www.netgear.com/docs .
---	--

Features of the HTML Version of this Manual

The HTML version of this manual includes these features.

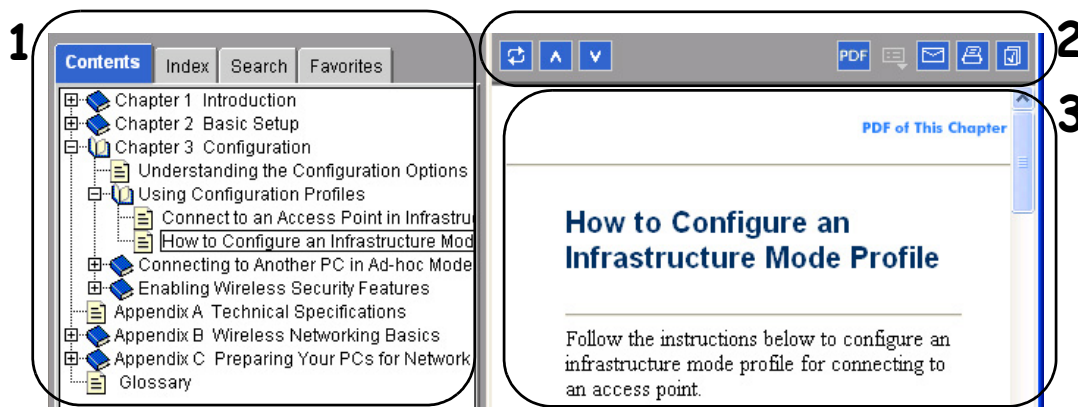


Figure Preface -2: HTML version of this manual

1. **Left pane.** Use the left pane to view the Contents, Index, Search, and Favorites tabs.

To view the HTML version of the manual, you must have a version 4 or later browser with JavaScript enabled.

2. **Toolbar buttons.** Use the toolbar buttons across the top to navigate, print pages, and more.

-  The *Show in Contents* button locates the current topic in the Contents tab.
-  *Previous/Next* buttons display the previous or next topic.
-  The *PDF* button links to a PDF version of the full manual.
-  The *Print* button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer—you do not have to worry about specifying the correct range of pages.

3. **Right pane.** Use the right pane to view the contents of the manual. Also, each page of the manual includes a [PDF of This Chapter](#) link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a “How To” Sequence of Steps in the HTML View.** Use the *Print* button  on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer—you do not have to worry about specifying the correct range of pages.
- **Printing a Chapter.** Use the [PDF of This Chapter](#) link at the top right of any page.
 - Click “PDF of This Chapter” link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

Note: Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.
 - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.
- **Printing the Full Manual.** Use the PDF button in the toolbar at the top right of the browser window.
 - Click the PDF button  on the upper right of the toolbar. The PDF version of the chapter you were viewing opens in a browser window.
 - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2

Switch Management Overview

This chapter gives an overview of switch management, including the methods you can use to manage your NETGEAR GSM7224 Layer 2 Managed Switch.

- Management Access Overview
- SNMP Access
- Protocols

Scope

The GSM7224 Layer 2 Managed Switch software has two purposes:

- Assists attached hardware in switching frames, based on Layer 2 information contained in the frames.
- Provides a complete switch management portfolio for the network administrator.

Switch Management Overview

Fast Ethernet (FEN) and Gigabit Ethernet (GEN) switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. The GSM7224 Layer 2 Managed Switch provides a flexible solution to these ever-increasing needs.

The GSM7224 Layer 2 Managed Switch provides the network administrator with a set of comprehensive management functions for managing both the GSM7224 and the network. The network administrator has a choice of three easy-to-use management methods:

- Web-based
- VT100 interface

Note: The maximum number of configuration file command lines is 2000.

- Simple Network Protocol Management (SNMP)

Each management method enables the network administrator to configure, manage, and control the GSM7224 locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private MIB providing control for functions not completely specified in the MIBs.

Table 2-1. Comparing Switch Management Methods

Management Method	Advantages	Disadvantages
Administration console	• Out-of-band access via direct cable connection means network bottlenecks, crashes, and downtime do not slow or prevent access • No IP address or subnet needed • Menu or CLI based • HyperTerminal access to full functionality (HyperTerminal are built into Microsoft Windows 95/98/NT/2000 operating systems) • Secure – make sure the switch is installed in a secure area.	• Must be near switch or use dial-up connection • Not convenient for remote users • Not graphical
Web browser or Telnet	• Can be accessed from any location via the switch's IP address • Ideal for configuring the switch remotely • Compatible with Internet Explorer and Netscape Navigator Web browsers • Familiar browser interface • Graphical data available • Most visually appealing • Menu or CLI interfaces available	• Security can be compromised (hackers can attack if they know IP address) • May encounter lag times on poor connections • Displaying graphical objects over a browser interface may slow navigation
SNMP Agent	• Communicates with switch functions at the Management Information Base (MIB) level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Limited amount of information available • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Chapter 3

Command Line Interface Syntax

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

Format

Commands are followed by values, parameters or both.

Example 1

config network parms <ipAddr> <netmask> [gateway]

- **config network parms** is the command name.
- **<ipAddr> <netmask>** are the required values for the command.
- **[gateway]** is the optional value for the command.

Example 2

config syslocation <location>

- **config syslocation** is the command name.
- **<location>** is the required parameter for the command.

Example 3

config lag deleteport <logical slot.port> <slot.port|all>

- **config lag deleteport** is the command name.
- **<logical slot.port> <slot.port|all>** are the required values for the command.

Command

The text in bold, non-italic font must be typed exactly as shown.

Parameters

Parameters are order dependent.

The text in bold italics should be replaced with a name or number. To use spaces as part of a name parameter, enclose it in double quotes like this: "System Name with Spaces".

Parameters may be mandatory values, optional values, choices or a combination.

- **<parameter>**. The <> angle brackets indicate that a mandatory parameter must be entered in place of the brackets and text inside them.
- **[parameter]**. The [] square brackets indicate that an optional parameter must be entered in place of the brackets and text inside them.
- **choice1|choice2**. The | slash indicates that only one of the parameters should be entered.

Values

ipAddr

This parameter is a valid IP address, made up of four decimal bytes ranging from 0 to 255. The default for all IP parameters consists of zeros and a one (that is, 0.0.0.1). The interface IP address of 0.0.0.0 is invalid. In some cases, the IP address can also be entered as a 32-bit number.

macAddr

The MAC address format is six hexadecimal numbers separated by colons, for example, 0:6:29:32:81:40.

areaId

Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network number of the subnetted network may be used for the area ID.

routerid

The value of **<router id>** must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

slot.port

This parameter denotes a valid slot number and a valid port number. For example, 0.1 represents slot number 0 and port

logical slot.port

number 1. The <slot.port> field is composed of a valid slot number and a valid port number separated by a period (.). This parameter denotes a logical slot number and logical port number assigned. This is applicable in the case of a LAG. The operator can use the logical slot number and the logical port number to configure the LAG.

Conventions

Network address are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:

Table 1. Network Address Syntax

Address Type	Format	Range
ipAddr	A.B.C.D	0.0.0.0 to 255.255.255.255 (decimal)
macAddr	YY:YY:YY:YY:YY:YY	hexidecimal digit pairs

Double quotation marks such as "System Name with Spaces" set off user-defined strings. If the operator wants to use spaces as part of a name parameter, then it must be enclosed in double quotation marks.

Entering '@' in front of any command allows the user to reference any root command from anywhere in the tree. For example, '>config router>@show arp table' displays the ARP table even though the command was not executed from the root level.

Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.

The value of '-----' designates that the value is unknown.

Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point ('!') character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character '!' is recognized as a comment line and ignored by the parser.

Some examples are provided below:

! Script file for displaying the ip interface

! Display information about interfaces

show ip interface 0.1 !Displays the information about the first interface

! Display information about the next interface

show ip interface 0.2

! End of the script file

Chapter 4

Administration Console Telnet Interface

The administration console is an internal, character-oriented, VT-100/ANSI menu-driven user interface for performing management activities. Using this method, you can view the administration console from a terminal, PC, Apple Macintosh, or UNIX workstation connected to the switch's console port. [Figure 4-1](#) shows an example of this management method.

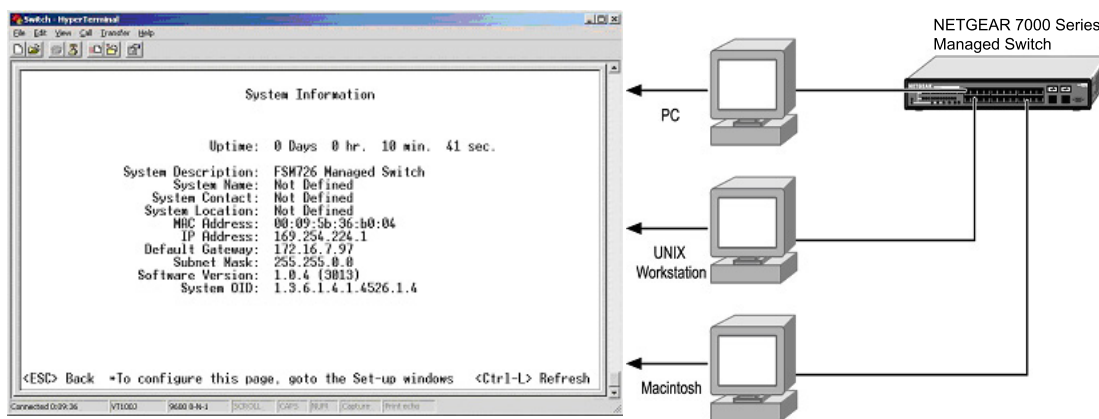


Figure 4-1: Administration Console Management Method

Set Up Your Switch Using Direct Console Access

The direct access management method is required when you initially set up your switch. Thereafter, the convenience and additional features of the Web management access method make it the best method to manage the switch. See [“Web Based Management Overview” on page 5-1](#) for more information.

Direct access to the switch console is achieved by connecting the switch's console port to a VT-100 or compatible terminal or to a PC, Apple Macintosh, or UNIX workstation equipped with a terminal-emulation program. This connection is made using the null-modem cable supplied with the switch.

Examples of terminal-emulation programs include:

- HyperTerminal, which is included with Microsoft Windows operating systems
- ZTerm for the Apple Macintosh
- TIP for UNIX workstations

This example describes how to set up the connection using HyperTerminal on a PC, but other systems follow similar steps.

1. Click the Windows Start button. Select Accessories and then Communications. HyperTerminal should be one of the options listed in this menu. Select HyperTerminal.
2. The following screen appears. Enter a name for this connection. In the example below, the name of the connection is FSM726. Click OK.



Figure 4-2: Connection Description

3. The following screen appears. In the bottom, drop down box labeled **Connect Using:**, click the arrow and choose the COM port to which the switch connects. In the example below, COM1 is the port selected. Click **OK**.



Figure 4-3: COM Port Selection

4. When the following screen appears, make sure that the port settings are as follows:

Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

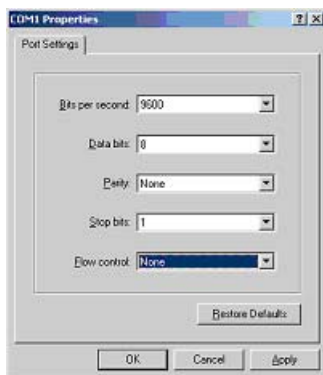


Figure 4-4: Connection Settings

5. Click OK.

The HyperTerminal window opens and you should be connected to the switch. If you do not get a welcome screen or a system menu, hit the return key.

When attached to the User Interface via a Telnet Session, the following must be set in order to use the arrow keys: Under the terminal pull down menu, choose Properties and make sure the VT100 Arrows option is turned on.

Chapter 5

Web-Based Management Interface

Your NETGEAR GSM7224 Layer 2 Managed Switch provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

This interface also allows for system monitoring and management of the switch. The 'help' page covers many of the basic functions and features of the switch and its web interface.

When you configure the switch for the first time from the console, you can assign an IP address and subnet mask to the switch. Thereafter, you can access the switch's Web interface directly using your Web browser by entering the switch's IP address into the address bar. In this way, you can use your Web browser to manage the switch from a central location, just as if you were directly connected to the switch's console port. Figure 4-1 shows this management method.

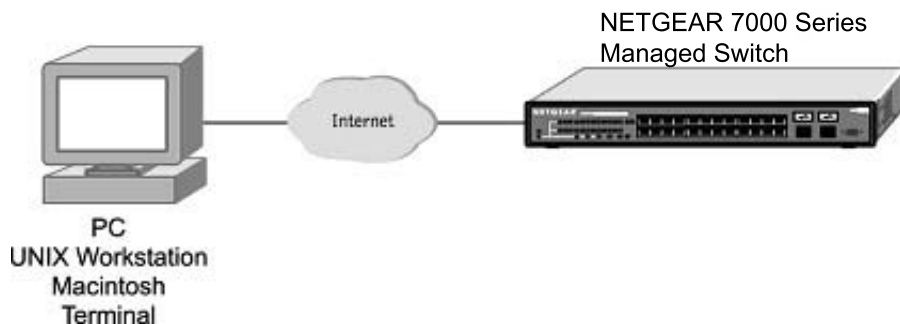


Figure 5-1: Web Management Method

Web Based Management Overview

The 6 menu options available are: System, Status, Set-up, Tools, Security, and Advanced. There is a help menu in the top of right side of screen; you can click the 'help' or the question mark to read the help menu.

The help menu contains:

- Web-Based Management Introduction to the Web management features.

- Device Management Introduction of the basic icons and management of the device
- Interface Operations Describes Web browser requirements, and common commands
- Product Overview Describes supported SNMP and Web management features
- Summary of Features Feature List

How to Log In to the GSM7224

The GSM7224 Layer 2 Managed Switch can be configured remotely from Microsoft Internet Explorer browser version 5.0 or above, or Netscape Navigator web browser version 4.78 or above.

1. Determine the IP address of your GSM7224.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Log in to the GSM7224 using the IP address the unit is currently configured with. Use the default user name of **admin** and default of no password, or whatever LAN address and password you have set up.



Figure 5-2: GSM7224 IP address in browser address bar

A login window opens:

Click the Login link.

A user name and password dialog box opens like this one.



Figure 5-3: User name/password dialog box

4. Type the default user name of **admin** and default of no password, or whatever password you have set up.

Once you have entered your access point name, your Web browser should automatically find the GSM7224 L2 Switch and display the home page, as shown below.

Web-Based Management Utility Features

This welcome page displays system information, such as:

- System Description
- System Name
- System Location
- System Contact
- IP Address
- System Object ID (OID)
- System Up Time

Interactive Switch Image

This dynamic image shows various real time conditions about the switch, including the status, fan operation, power, and the connectivity and traffic indication for each port. In addition, using the popup menus described below, you can directly access a wealth of information by right-clicking on a port and selecting a menu item from the popup-menu that displays.

Menus

The Web-based interface enables navigation through several menus. The main navigation menu is on the left of every page and contains the screens that let you access all the commands and statistics the switch provides.

The main menus are:

- System
- Switching
- QoS

System-Wide Popup Menus

The GSM7224 L2 Switch also provides several popup menus.

You can also access the main navigation menu by right clicking on the image of the switch and browsing to the menu you want to use.

Port-Specific Popup Menus

The GSM7224 L2 Switch also provides several popup menus for each port.

You can access a port-specific popup menu by right clicking on the port in the image of the switch and browsing to the menu you want to use.

Chapter 6

Quick Startup

The Command Line Interface Quick Startup chapter details procedures to quickly become acquainted with the GSM7224 Layer 2 Managed Switch software.

This chapter contains the following Quick Startup examples:

- [“System Info and System Setup” on page 6-2](#)
- [“VLAN Configuration Example” on page 6-8](#)

Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the GSM7224 L2 Switch software locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).
2. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
3. When the prompt asks for operator login, execute the following steps:
 - Type the word **admin** in the login area. Since a number of the Quick Setup commands require administrator account rights, log in using an administrator account.
 - Do not enter a password because there is no password in the default mode.
 - Press the enter key two times.

System Info and System Setup

There are several categories of Quick Startup commands:

- “Quick Startup Software Version Information” on page 6-2
- “Quick Startup Physical Port Data” on page 6-3
- “Quick Startup User Account Management” on page 6-3
- “Quick Startup IP Address” on page 6-4
- “Quick Startup Uploading from Switch to Out-of-Band PC (Only XMODEM)” on page 6-6
- “Quick Startup Downloading from Out-of-Band PC to Switch (Only XMODEM)” on page 6-6
- “Quick Startup Downloading from TFTP Server” on page 6-7
- “Quick Startup Factory Defaults” on page 6-7

Quick Startup Software Version Information

Table 6-1. Quick Startup Software Version Information

Command	Details
show inventory	Allows the user to see the software version the device contains
	Machine Model (The type and number of ports the device provides.)
	For example: System Description netgear Burned In MAC Address 00:06:29:32:81:40 Software Version 1.0.0.9

Quick Startup Physical Port Data

Table 6-2. Quick Startup Physical Port Data

Command	Details
show port all	Displays the Port Characteristics
	Slot.Port - slot number.port number Slot Options: 0 - the port is one of the physical ports 1 - a link aggregation group (LAG). The port number field in this case refers to the LAG group ID. 3 - a VLAN group. The port field starts with 1 as the first VLAN group created in the switch.
	Port (when Slot value is 0): Ports 1-24 are gigabit copper ports, ports 21-24 can also be used as fiber ports
	Type - indicates if the port is a special type of port
	STP State - displays the Spanning Tree status
	Admin Mode - selects the Port Control Administration State
	Physical Mode - selects the desired port speed and duplex mode
	Physical Status - indicates the port speed and duplex mode
	Link Status - indicates whether the link is up or down
	Link Trap - determines whether or not to send a trap when link status changes
	LACP Mode - displays whether LACP is enabled or disabled on this port.

Quick Startup User Account Management

Table 6-3. Quick Startup User Account Management

Command	Details
show users	Displays all of the users that are allowed to access the switch
	Access Mode - Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view then (Read Only). As a factory default, admin has Read/Write access and guest has Read Only access. There can only be one Read/Write user and up to 5 Read Only users.

Table 6-3. Quick Startup User Account Management

Command	Details
show login session	Displays all of the login session information
config users passwd <user>	Allows the user to set passwords or change passwords needed to log in. A prompt appears requesting the users old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command. The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message is displayed.
save config	This command saves passwords and all other changes to the device. If you do not issue this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.
logout	Logs the user out of the switch

Quick Startup IP Address

To view the network parameters the operator can access the device by the following three methods.

- Simple Network Management Protocol - SNMP
- Telnet
- Web browser

Note: Helpful Hint - do a save config after changing the network parameters so that the configurations are not lost.

Table 6-4. Quick Startup IP Address

Command	Details
show network	Displays the Network Configurations
	IP Address - IP Address of the interface Default IP is 0.0.0.0
	Subnet Mask - IP Subnet Mask for the interface Default is 0.0.0.0

Table 6-4. Quick Startup IP Address

Command	Details
	Default Gateway - The default Gateway for this interface Default value is 0.0.0.0
	Burned in MAC Address - The Burned in MAC Address used for in-band connectivity
	Locally Administered MAC Address - Can be configured to allow a locally administered MAC address
	MAC Address Type - Specifies which MAC address should be used for in-band connectivity
	Network Configurations Protocol Current - Indicates which network protocol is being used Default is DHCP
	Java Mode - Specifies whether the switch should allow the Java applet to show the interactive switch graphic (see “Interactive Switch Image” on page 5-3) Default is enable
config network parms	config network parms <ipAddr> <Mask> <gateway>
	IP Address range from 0.0.0.0 to 255.255.255.255
	Subnet Mask range from 0.0.0.0 to 255.255.255.255
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Quick Startup Uploading from Switch to Out-of-Band PC (Only XMODEM)

Table 6-5. Quick Startup Uploading from Switch to Out-of-Band PC (Only XMODEM)

Command	Details
transfer upload mode xmodem	Changes mode to xmodem which is initiated by the serial EIA 232 port
transfer upload datatype <config errorlog systemtrace traplog>	The types are: config - configuration file errorlog - error log system trace - system trace traplog - trap log
transfer upload start	This starts the upload and also displays the mode of uploading and the type of upload it is and confirms the upload is taking place. For example: If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.

Quick Startup Downloading from Out-of-Band PC to Switch (Only XMODEM)

Table 6-6. Quick Startup Downloading from Out-of-Band PC to Switch (Only XMODEM)

Command	Details
transfer download mode xmodem	Makes the download mode to be xmodem
transfer download datatype <config/code>	Sets the download datatype to be an image or config file. The default is a code file.
transfer download start	For example: If the user is using HyperTerminal, the user must specify which file is to be sent to the switch. The Switch restarts automatically once the code has been downloaded.

Quick Startup Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Startup for the IP Address.

Table 6-7. Quick Startup Downloading from TFTP Server

Command	Details
transfer download mode TFTP	Makes the download mode to be TFTP
transfer download datatype <config/code>	Sets the download datatype to be an image or config file. The default is a code file.
transfer download filename <name>	The name can ONLY be an image file or a configuration file of the switch.
transfer download serverip <ipAddr>	The IP Address is the source IP Address.
transfer download start	Starts the TFTP download

Quick Startup Factory Defaults

Table 6-8. Quick Startup Factory Defaults

Command	Details
clear config	Enter yes when the prompt pops up to clear all the configurations made to the switch.
save config	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
reset system OR Cold Boot the Switch	Enter yes when the prompt pops up that asks if you want to reset the system. This is the users choice either reset the switch or cold boot the switch, both work effectively.

VLAN Configuration Example

This section provides configuration examples for VLAN configurations.

LAN switches can segment networks into logically defined virtual workgroups. This logical segmentation is commonly referred to as a virtual LAN (VLAN). This logical segmentation of devices provides better LAN administration, security, and management of broadcast activity over the network. Virtual LANs have become an integral feature of switched LAN solutions.

The VLAN example below demonstrates a simple VLAN configuration with a GSM7224 Layer 2 Managed Switch.

If a single port is a member of VLANs 2, 3 and 4, the port expects to see traffic tagged with either VLAN 2, 3 or 4.

The PVID (Port Virtual Identification) could be something entirely different, for example '12' and things would still work fine, just so incoming traffic was tagged.

Example:

- Project A = (VLAN2, ports 1,2)
- Project B = (VLAN3, ports 3,4)
- Project C = (VLAN4, ports 5,6)
- Project P = (VLAN 9, port 7)

Table 6-9. Creating the VLANs

VLAN	Command
create VLAN 2	<pre>config vlan create 2 config vlan participation include 2 0.1 config vlan participation include 2 0.2</pre>
create VLAN 3	<pre>config vlan create 3 config vlan participation include 3 0.3 config vlan participation include 3 0.4</pre>

Table 6-9. Creating the VLANs

VLAN	Command
create VLAN 4	<pre>config vlan create 4 config vlan participation include 4 0.5 config vlan participation include 4 0.6</pre>
create VLAN 9	<pre>config vlan create 9 config vlan participation include 9 0.1 config vlan participation include 9 0.2 config vlan participation include 9 0.3 config vlan participation include 9 0.4 config vlan participation include 9 0.5 config vlan participation include 9 0.6 config vlan participation include 9 0.7</pre>

Solution 1

All traffic entering the ports is tagged traffic. Since the traffic is tagged, the PVID configuration for each port is not a concern. The network card configuration is as follows:

- Devices on Project A should tag all traffic with 'VLAN 2'
- Devices on Project B should tag all traffic with 'VLAN 3'
- Devices on Project C should tag all traffic with 'VLAN 4'
- Devices on Project P should tag all traffic with 'VLAN 9'

Solution 2

The network card configuration for devices on Project A, B and C should be set to NOT tag traffic.

To take care of these untagged frames configure the following:

- `config vlan ports pvid 2 0.1`
- `config vlan ports pvid 2 0.2`
- `config vlan ports pvid 3 0.3`
- `config vlan ports pvid 3 0.4`
- `config vlan ports pvid 4 0.5`
- `config vlan ports pvid 4 0.6`

Chapter 7

Switching Commands

This chapter provides detailed explanation of the Switching commands. The commands are divided into five functional groups:

- Show commands display switch settings, statistics, and other information.
- Config commands configure features and options of the switch. For every config command there is a show command that displays the config setting.
- Transfer commands transfer configuration and informational files to and from the switch.
- Save commands save the switch configuration.
- Clear commands clear some or all of the settings to factory defaults.

This chapter is organized by configuration type:

- [“System Information and Statistics Commands” on page 7-1](#)
- [“Management Commands” on page 7-13](#)
- [“Device Configuration Commands” on page 7-23](#)
- [“Spanning Tree Commands” on page 7-45](#)
- [“User Account Management Commands” on page 7-56](#)
- [“Security Commands” on page 7-58](#)
- [“System Utilities” on page 7-74](#)

System Information and Statistics Commands

These commands display and configure system information and statistics.

show inventory

This command displays inventory information for the switch.

Format	show inventory
--------	----------------

Switch Description	Text used to identify the product name of this switch.
Machine Type	Specifies the machine model as defined by the Vital Product Data.
Machine Model	Specifies the machine model as defined by the Vital Product Data.
Serial Number	The unique box serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Indicates hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.
Burnedin MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Operating System	The operating system currently running on the switch.
Network Processing Element	The type of the processor microcode.
Additional Packages	This displays the additional packages that are incorporated into this system, such as FASTPATH BGP-4, or FASTPATH Multicast.

show sysinfo

This command displays switch information.

Format	show sysinfo
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.
System Location	Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank.
System Contact	Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

config sysname

This command sets the name assigned to the switch. The range for the name is from 1 to 31 alphanumeric characters.

Default	Blank
Format	config sysname <name>

config syslocation

This command sets the physical location of the switch. The range for the name is from 1 to 31 alphanumeric characters.

Default	Blank
Format	config syslocation <location>

config syscontact

This command sets the organization responsible for the network. The range for the name is from 1 to 31 alphanumeric characters.

Default	Blank
Format	config syscontact <contact>

show arp switch

This command displays connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

Format	show arp switch
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example: 01:23:45:67:89:AB
IP Address	The IP address assigned to each interface.
Slot.Port	This parameter denotes a valid slot number and a valid port number.

show forwardingdb table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional *all* parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

Format	show forwardingdb table [macaddr/all]
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example, 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.

Slot.Port	The port which this address was learned.
if Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: Static - The value of the corresponding instance was added by the system or a user and cannot be relearned. Learned - The value of the corresponding instance was learned, and is being used. Management - The value of the corresponding instance is also the value of an existing instance of dot1d Static Address. Currently this is used when enabling VLANs for routing. Self - The value of the corresponding instance is the system's own MAC address. GMRP Learned - The value of the corresponding instance was learned via GMRP. Other - The value of the corresponding instance does not fall into one of the other categories.

show forwardingdb learned

This command displays the forwarding database entries for learned addresses. If the command is entered with no parameter, all learned addresses are displayed. This is the same as entering the optional *all* parameter. Alternatively, the administrator can enter a VLAN and MAC Address to display the table entry for the requested MAC address and all learned entries following the requested MAC address.

Format	show forwardingdb learned[vlanplusmacaddr/all]
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example, 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.
Slot.Port	The port which this address was learned.
if Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. This value will always be Learned.

show stats port detailed

This command displays detailed statistics for a specific port.

Format	show stats port detailed <slot.port>
Packets Received	

Octets Received - the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.

Packets Received < 64 Octets - the total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 64 Octets - the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 65-127 Octets - the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 128-255 Octets - the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 256-511 Octets - the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 512-1023 Octets - the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1024-1518 Octets - the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1519-1522 Octets - the total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received > 1522 Octets - the total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets Received Successfully

Total - the total number of packets received that were without errors.

Unicast Packets Received - the number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - the total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with MAC Errors

Total - the total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Jabbers Received - the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Fragments/Undersize Received - the total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).

Alignment Errors - the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors - the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Overruns - the total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets not forwarded

Total - a count of valid frames received which were discarded (i.e. filtered) by the forwarding process.

Local Traffic Frames - the total number of frames dropped in the forwarding process because the destination address was located off of this port.

802.3x Pause Frames Received - a count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - the number of frames discarded from this port due to being an unacceptable frame type.

VLAN Membership Mismatch - the number of frames discarded on this port due to ingress filtering.

VLAN Viable Discards - the number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Multicast Tree Viable Discards - the number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

Reserved Address Discards - the number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

Broadcast Storm Recovery - the number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

CFI Discards - the number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

Upstream Threshold - the number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

Total Bytes - the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.

Packets Transmitted 64 Octets - the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 65-127 Octets - the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 128-255 Octets - the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 256-511 Octets - the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 512-1023 Octets - the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1024-1518 Octets - the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1519-1522 Octets - the total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Max Info - the maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

Total - the number of frames that have been transmitted by this port to its segment.

Unicast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors

Total Errors - the sum of Single, Multiple, and Excessive Collisions.

FCS Errors - the total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Oversized - the total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.

Underrun Errors - the total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

Total Discards - the sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Single Collision Frames - a count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - a count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Excessive Collisions - a count of frames for which transmission on a particular interface fails due to excessive collisions.

Port Membership - the number of frames discarded on egress for this port due to egress filtering being enabled.

VLAN Viable Discards - the number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Protocol Statistics

BPDU's received - the count of BPDU's (Bridge Protocol Data Units) received in the spanning tree layer.

BPDU's Transmitted - the count of BPDU's (Bridge Protocol Data Units) transmitted from the spanning tree layer.

802.3x Pause Frames Received - a count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDU's Received - the count of GVRP PDU's received in the GARP layer.

GVRP PDU's Transmitted - the count of GVRP PDU's transmitted from the GARP layer.

GVRP Failed Registrations - the number of times attempted GVRP registrations could not be completed.

GMRP PDU's received - the count of GMRP PDU's received in the GARP layer.

GMRP PDU's Transmitted - the count of GMRP PDU's transmitted from the GARP layer.

GMRP Failed Registrations - the number of times attempted GMRP registrations could not be completed.

STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received

RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received

MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Dot1x Statistics

EAPOL Frames Received - the number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted - the number of valid EAPOL frames of any type that have been transmitted by this authenticator.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

show stats port summary

This command displays a summary of statistics for a specific port.

Format	show stats port summary <slot.port>
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

show stats switch detailed

This command displays detailed statistics for all CPU traffic.

Format

show stats switch detailed

Total Packets Received (Octets) - the total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Packets Received Without Error - the total number of packets (including broadcast packets and multicast packets) received by the processor.

Unicast Packets Received - the number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - the total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - the total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Receive Packets Discarded - the number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Octets Transmitted - the total number of octets transmitted out of the interface, including framing characters.

Packets Transmitted without Errors - the total number of packets transmitted out of the interface.

Unicast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - the total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded - the number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Most Address Entries Ever Used - the highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

Address Entries in Use - the number of Learned and static entries in the Forwarding Database Address Table for this switch.

Maximum VLAN Entries - the maximum number of Virtual LANs (VLANs) allowed on this switch.

Most VLAN Entries Ever Used - the largest number of VLANs that have been active on this switch since the last reboot.

Static VLAN Entries - the number of presently active VLAN entries on this switch that have been created statically.

Dynamic VLAN Entries - the number of presently active VLAN entries on this switch that have been created by GVRP registration.

VLAN Deletes - the number of VLANs on this switch that have been created and then deleted since the last reboot.

**Time Since Counters
Last Cleared**

The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

show stats switch summary

This command displays a count of all CPU traffic.

Format

show stats switch summary

**Packets Received
Without Error**

The total number of packets (including broadcast packets and multicast packets) received by the processor.

**Broadcast Packets
Received**

The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Packets Received
With Error**

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

**Packets Transmitted
Without Error**

The total number of packets transmitted out of the interface.

**Broadcast Packets
Transmitted**

The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

**Transmit Packet Errors
Address Entries
Currently In Use**

The number of outbound packets that could not be transmitted because of errors.

The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

**VLAN Entries
Currently In Use
Time Since Counters
Last Cleared**

The number of VLAN entries presently occupying the VLAN table.

The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format	show eventlog
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

Note: Event log information is retained across a switch reset.

show msglog

This command displays the message log maintained by the switch. The message log contains system trace information.

The trap log contains a maximum of 256 entries that wrap.

Format	show msglog
Message	The message that has been logged.

Note: Message log information is not retained across a switch reset.

show traplog

This command displays the trap log maintained by the switch.

The trap log contains a maximum of 256 entries that wrap.

Format	show traplog
Number of Traps since last reset	The number of traps that have occurred since the last reset of this device.
Number of Traps since log last displayed	The number of traps that have occurred since the traps were last displayed. Getting the traps by any method (terminal interface display, Web display, upload file from switch etc.) will result in this counter being cleared to 0.
Log	The sequence number of this trap.
System Up Time	The relative time since the last reboot of the switch at which this trap occurred.
Trap	The relevant information of this trap.

Note: Trap log information is not retained across a switch reset.

Management Commands

These commands manage the switch and show current management settings.

show network

This command displays network configuration settings that are vital for switch operation.

Format	show network
IP Address	The IP address of the interface. The factory default value is 0.0.0.0
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0
BurnedIn MAC Address	The burnedin MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	Specifies which MAC address should be used for in-band connectivity. The choices are the burnedin or the Locally Administered address. The factory default is to use the burnedin MAC address.
Network Configuration Protocol Current	Indicates which network protocol is being used. The options are bootp dhcp none.
Web Mode	Specifies if the switch should allow access from a web browser. Enabled means the switch can be managed from a web browser. The factory default is enabled.
Java Mode	Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is enabled.

config network macaddr

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').

- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macAddr, must be 2, 6, A or E.
A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format `config network macaddr <macAddr>`

config network mactype

This command specifies whether the burnedin MAC address or the locally-administered MAC address is used.

Default burnedin
Format `config network mactype <local|burnedin>`

config network parms

This command sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.

Format `config network parms <ipAddr> <netmask> [gateway]`

config network protocol

This command specifies the network configuration protocol to be used. If you modify this value change is effective immediately. See “save config” on page 74 for more information.

Default none
Format `config network protocol <none|bootp|dhcp>`, where **bootp** indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a dhcp server until a response is received. **none** indicates that the switch should be manually configured with IP information.

config network webmode

This command enables or disables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Disabling the Web interface takes effect immediately. All interfaces are effected.

Default	enable
Format	config network webmode <enable disable>

config network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

Default	enable
Format	config network javamode <enable disable>

config prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Default	<model #>
Format	config prompt <system prompt>

show serial

This command displays serial communication settings for the switch.

Format	show serial
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate	The default baud rate at which the serial port will try to connect. This is selected from a pull-down menu. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory Default is 9600 baud.
Character Size	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

config serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default	9600
Format	config serial baudrate <speed>

config serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default	5
Format	config serial timeout <0 - 160>

show serviceport

This command displays service port configuration information.

Format	show serviceport
IP Address	The IP address of the interface. The factory default value is 0.0.0.0
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0
ServPort Configuration Protocol Current	Indicates what network protocol was used on the last, or current power-up cycle, if any.
Burnedin MAC Address	The burnedin MAC address used for in-band connectivity.

config serviceport parms

This command sets the IP address, the netmask and the gateway of the router.

Format	config serviceport parms <ipAddr> <netmask> [gateway]
---------------	--

config serviceport protocol

This command specifies the servicePort configuration protocol. If you modify this value, the change takes effect immediately.

Format	config serviceport protocol <none bootp dhcp>
---------------	--

show snmpcommunity

This command displays SNMP community information.

Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format	show snmpcommunity
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note: that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0
Access Mode	The access level for this community string. May be specified by selecting Read/Write or Read Only from the pull-down. Updates will be made to the switch by pressing the Submit button.
Status	The status of this community access entry. When this object is set to enabled, if the Community Name for this row is not unique among all valid rows, the set request will be rejected. Community names may be made invalid by selecting disable. Rows may be deleted by selecting Delete. Updates will be made to the switch by pressing the Submit button.

config snmpcommunity accessmode

This command restricts access to switch information. The access mode can be read-only (also called public) or read/write (also called private).

Format	config snmpcommunity accessmode <ro rw> <name>
---------------	---

config snmpcommunity create

This command adds (and names) a new SNMP community. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 16 case-sensitive characters.

Note: Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default	Two default community names: Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.
Format	config snmpcommunity create <name>

config snmpcommunity delete

This command removes this community name from the table. The name is the community name to be deleted.

Format	config snmpcommunity delete <name>
---------------	---

config snmpcommunity ipaddr

This command sets an IP address for an SNMP community. The address is the associated community SNMP packet sending address. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Default	0.0.0.0
Format	config snmpcommunity ipaddr <ipAddr> <name>

config snmpcommunity ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Default	0.0.0.0
Format	config snmpcommunity ipmask <ipmask> <name>

config snmpcommunity mode

This command activates or deactivates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default	The default private and public communities are enabled by default. The four undefined communities are disabled by default.
Format	config snmpcommunity mode <enable disable> <name>

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format	show snmptrap
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. This may be up to 16 alphanumeric characters. This string is case sensitive.
IP Address	The IP address to receive SNMP traps from this device. Enter 4 numbers between 0 and 255 separated by periods.
Status	A pull down menu that indicates the receiver's status(enabled or disabled) and allows the administrator/user to perform actions on this user entry: Enable - send traps to the receiver. Disable - do not send traps to the receiver. Delete - remove the table entry.

config snmptrap create

This command adds an SNMP trap name. The maximum length of name is 16 case-sensitive alphanumeric characters.

Default	The default name for the six undefined community names is Delete.
Format	config snmptrap create <name> <ipAddr>

config snmptrap delete

This command deletes trap receivers for a community.

Format	config snmptrap delete <name> <ipaddr>
---------------	---

config snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format `config snmptrap ipaddr <ipaddrold> <name> <ipaddrnew>`

config snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format `config snmptrap mode <enable|disable> <name> <ipaddr>`

show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Authentication Flag	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled. Indicates whether authentication failure traps will be sent.
----------------------------	---

Link Up/Down Flag	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled. Indicates whether link status traps will be sent. Multiple Users Flag.
--------------------------	---

Multiple Users Flag	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).
----------------------------	--

Spanning Tree Flag	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled. Indicates whether spanning tree traps will be sent.
---------------------------	--

Broadcast Storm Flag	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled. Indicates whether broadcast storm traps will be sent.
-----------------------------	--

config trapflags authentication

This command enables or disables the Authentication Flag.

Default	enable
Format	config trapflags authentication <enable disable>

config trapflags bcaststorm

This command enables or disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled (see “config switchconfig broadcast” on page 24).

Default	enable
Format	config trapflags bcaststorm <enable disable>

config trapflags linkmode

This command enables or disables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see “config port linktrap” on page 26).

Default	enable
Format	config trapflags linkmode <enable disable>

config trapflags multiusers

This command enables or disables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or telnet) and there is an existing terminal interface session.

Default	enable
Format	config trapflags multiusers <enable disable>

config trapflags stpmode

This command enables or disables the sending of new root traps and topology change notification traps.

Default	enable
Format	config trapflags stpmode <enable disable>

show telnet

This command displays telnet settings.

Format	show telnet
Telnet Login Timeout (minutes)	This object indicates the number of minutes a telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
Maximum Number of Telnet Sessions	Selectable from a pull-down menus for values of from 0 to 5. This object indicates the number of simultaneous telnet sessions allowed. The factory default is 5.
Allow New Telnet Sessions	Indicates that new telnet sessions will not be allowed when set to no. The factory default value is yes.

config telnet maxsessions

This command specifies the maximum number of telnet sessions that can be established. A value of 0 indicates that no telnet session can be established. The range is 0 to 5.

Default	5
Format	config telnet maxsessions <0-5>

config telnet mode

This command regulates new telnet sessions. If sessions are enabled, new telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends it.

Default	enable
Format	config telnet mode <enable disable>

config telnet timeout

This command sets the telnet session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. the time is a decimal value from 0 to 160.

Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Default	5
Format	config telnet timeout <0-160>

show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid|all] parameter is required. In an SVL system, the [fdbid|all] parameter is not used and will be ignored if entered.

Default	<i>all</i>
Format	show forwardingdb agetime [fdbid all]
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system. This field will not be displayed in an SVL system.
Agetime	displays the address aging timeout for the associated forwarding database in IVL. In an SVL system, this will display the system's address aging timeout value in seconds.

config forwardingdb agetime

This command configures the forwarding database address aging timeout. In an IVL system, the [fdbid/all] parameter is required. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Default	The default value for <10-1,000,000> is 300 seconds
Format	config forwardingdb agetime <10-1,000,000> [fdbid/all]
Seconds	The <seconds> parameter must be within the range of 10 to 1,000,000 seconds.
Forwarding Database ID	Fdbid (Forwarding database ID) indicates which forwarding database's aging timeout is being configured. All is used to configure all forwarding database's agetime. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Device Configuration Commands

This section describes device configuration commands.

show switchconfig

This command displays switch configuration information.

Format	show switchconfig
Broadcast Storm Recovery Mode	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is disabled.
802.3x Flow Control Mode	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is disabled.

config switchconfig broadcast

This command enables or disables broadcast storm recovery mode. If the mode is enabled, broadcast storm recovery with high and low thresholds is implemented.

The threshold implementation follows a percentage pattern. If the broadcast traffic on any Ethernet port exceeds the high threshold percentage (as represented in “Broadcast Storm Recovery Thresholds” table) of the link speed, the switch discards the broadcasts traffic until the broadcast traffic returns to the low threshold percentage or less. The full implementation is depicted in the “Broadcast Storm Recovery Thresholds” table.

Table 2. Broadcast Storm Recovery Thresholds

Link Speed	High	Low
10M	20	10
100M	5	2
1000M	5	2

Format	config switchconfig broadcast <enable/disable>
---------------	---

config switchconfig flowcontrol

This command enables or disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Default	enable
Format	config switchconfig flowcontrol <enable/disable>

show port

This command displays port information.

Format	show port <slot.port all>
Slot.Port	The physical slot and physical port.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: Mon - this port is a monitoring port. Look at the Port Monitoring screens to find out more information. Lag - this port is a member of a Lag. Look at the Lag screens to find out more information. Probe - this port is a probe port. Look at the Port Mirroring screens to find out more information.
Admin Mode	Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Physical Mode	Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.

config port adminmode

This command enables or disables a port.

Default	enable
Format	config port adminmode <slot.port all> <enable disable>

config port flowcontrol

This command enables or disables flow control on the specified interface.

Format	config port flowcontrol <slot.port all> <enable disable>
---------------	---

config port linktrap

This command enables or disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “config trapflags linkmode” on page 21 for more information.

Format	config port linktrap < slot.port all> <enable disable>
---------------	---

config port physicalmode

This command sets the speed and duplex setting for the interface.

Format	config port physicalmode <slot.port all> <100h 100f 10h 10f>
---------------	---

Acceptable values are:

100h	100BASE-T half-duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	100BASE-T full duplex

config port lacpmode

This command enables or disables Link Aggregation Control Protocol (LACP) on a port. The possible values for <mode> are enable and disable. The default value is disable.

Format	config port lacpmode <slot.port/all> <enable/disable>
---------------	--

config port autoneg

This command enables or disables automatic negotiation on a port. The possible values for <mode> are enable and disable. The default value is enable.

Format	config port autoneg <slot.port/all> <enable/disable>
---------------	---

show lag

This command displays an overview of all link aggregations (LAGs) on the switch.

Format	show lag <logical slot.port all>
---------------	---

Logical Slot.Port	The logical slot and the logical port.
Lag Name	The name of this lag. You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Link Trap Mode	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port or lag. The possible values are: Disable - Spanning tree is disabled for this port. Enable - Spanning tree is enabled for this port.
Mbr Ports	A listing of the ports that are members of this lag, in slot.port notation. There can be a maximum of 8 ports assigned to a given lag.
Port Speed	

config lag create

This command configures a new LAG and generates a logical slot and port number for it. Display this number using the “show lag” on page 26.

Note: Before including a port in a LAG, set the port physical mode. See “config port physicalmode” on page 26.

Format `config lag create <name>`

config lag addport

This command adds one port to the LAG. The first interface is a logical slot and port number of a configured LAG.

Note: Before adding a port to a LAG, set the physical mode of the port. See “config port physicalmode” on page 26.

Format `config lag addport <logical slot.port> <slot.port>`

config lag deleteport

This command deletes one or more ports from the LAG. The first interface is a logical slot and port number of a configured LAG, and the second interface is a valid slot and port number that is a member of any LAG or **all** (to delete all ports in the specified LAG).

Format `config lag deleteport <logical slot.port>
<slot.port|all>`

config lag adminmode

This command enables or disables a LAG. The interface is a logical slot and port for a configured LAG. The option **all** sets every configured LAG with the same administrative mode setting.

Format	config lag adminmode <logical slot.port all> <enable disable>
---------------	--

config lag linktrap

This command enables or disables link trap notifications for the LAG. The interface is a logical slot and port for a configured LAG. The option **all** sets every configured LAG with the same administrative mode setting.

Default	enable
Format	config lag linktrap <logical slot.port all> <enable disable>

config lag name

This command defines a name for the LAG. The interface is a logical slot and port for a configured LAG, and name is an alphanumeric string up to 15 characters. This command is used to modify the name that was associated with the LAG when it was created.

Format	config lag name <logical slot.port all> <name>
---------------	---

config lag deletelag

This command deletes an existing lag from the configuration. The interface is a logical slot and port for a configured LAG. The **all** option removes all configured LAGs.

Format	config lags deletelag <logical slot.port all>
---------------	--

config lag stpmode

This command sets the STP mode for a specific LAG. This is the value specified for STP Mode on the Port Configuration Menu. 802.1D mode is the default. The interface is a logical slot and port for a configured LAG. The **all** option sets all configured LAGs with the same option.

Format	config lag stpmode <logical slot.port all> <off 802.1d fast>
---------------	---

The mode is one of the following:

802.1d	IEEE 802.1D-compliant STP mode is used.
fast	Fast STP mode is used.
off	STP is turned off.

show vlan summary

This command displays a list of all configured VLANs.

Format	show vlan summary
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.
VLAN Type	What type of VLAN this is. A VLAN can be the Default VLAN, (VLAN ID = 1), a static VLAN, one that is configured and permanently defined, or a Dynamic VLAN, one that is created by GVRP registration. In order to change a VLAN from Dynamic to Static, select Static from the Vlan Type pull-down entry field. Once the VLAN is selected, click on Submit. This will change the VLAN type to Static.

show vlan detailed

This command displays detailed information, including interface information, for a specific VLAN.

Format	config vlan detailed <vlan id> , where the ID is a valid VLAN identification number
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.
VLAN Type	What type of VLAN this is. A VLAN can be the Default VLAN, (VLAN ID = 1), a static VLAN, one that is configured and permanently defined, or a Dynamic VLAN, one that is created by GVRP registration. In order to change a VLAN from Dynamic to Static, select Static from the Vlan Type pull-down entry field. Once the VLAN is selected, click on Submit. This will change the VLAN type to Static.
Slot.Port	Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.

Current

Determines the degree of participation of this port in this VLAN. The permissible values are:

Include - this port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude - this port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect - Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured

Determines the configured degree of participation of this port in this VLAN. The permissible values are:

Include - this port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude - this port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect - specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging

Select the tagging behavior for this port in this VLAN.

Tagged - specifies to transmit traffic for this VLAN as tagged frames.

Untagged - specifies to transmit traffic for this VLAN as untagged frames.

config vlan create

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN) VLAN range is 2-4094.

Format

config vlan create <2-4094>

config vlan delete

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN) VLAN range is 2-4094.

Format

config vlan delete <2-4094>

config vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 16 characters, and the ID is a valid VLAN identification number. ID range is 1-4094.

Default	The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.
Format	config vlan name <name> <2-4094>

config vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4094.

Format	config vlan makestatic <2-4094>
---------------	--

config vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number or **all**.

Format	config vlan participation <exclude include auto> <1-4094> <slot.port all>
---------------	--

Participation options are:

include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

config vlan port tagging

This command configures the tagging behavior for a specific interface in a VLAN. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number. The interface is a valid port number or **all**.

Format	config vlan port tagging <enable disable> <1-4094> <slot.port all>
---------------	---

show vlan port

This command displays VLAN port information.

Format	show vlan port <slot.port>
Slot.Port	Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	Specifies the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled by selecting the corresponding line on the pull-down entry field. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	

config vlan port pvid

This command changes the VLAN ID per interface.

Default	1
Format	config vlan port pvid <1-4094> <slot.port all>

config vlan port acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification. VLAN ID range is 1-4094.

Default	Admit All
----------------	-----------

Format	config vlan port acceptframe <all vlan> <slot.port all>
---------------	--

config vlan port ingressfilter

This command enables or disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disable
Format	config vlan port ingressfilter <enable disable> <slot.port all>

show protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated Group.

Format	show protocol detailed <groupid/all>
Group Name	This field displays the group name of an entry in the Protocol-based VLAN table.
Group ID	This field displays the group identifier of the protocol group.
Protocol(s)	This field indicates the type of protocol(s) for this group.
VLAN	This field indicates the VLAN associated with this Protocol Group.
Interface(s)	This field lists the Slot.Port interface(s) that are associated with this Protocol Group.

config protocol create

This command adds protocol-based VLAN group to the system. The <groupName> is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format	config protocol create <groupname>
---------------	---

config protocol delete

This command removes the protocol-based VLAN group that is identified by this <groupid>.

Format	config protocol delete <groupid>
---------------	---

config protocol protocol add

This command adds the <protocol> to the protocol-based VLAN identified by <groupid>. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are *ip*, *arp*, and *ipx*.

Default	none
Format	config protocol protocol add <groupid> <protocol>

config protocol protocol remove

This command removes the <protocol> from this protocol-based VLAN group that is identified by this <groupid>. The possible values for protocol are *ip*, *arp*, and *ipx*.

Default	none
Format	config protocol protocol remove <groupid> <protocol>

config protocol vlan add

This command attaches a <vlan> to the protocol-based VLAN identified by <groupid>. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	none
Format	config protocol vlan add <groupid> <vlan>

config protocol vlan remove

This command removes the <vlan> from this protocol-based VLAN group that is identified by this <groupid>.

Default	none
Format	config protocol vlan remove <groupid> <vlan>

config protocol interface add

This command adds the physical `<slot.port>` interface to the protocol-based VLAN identified by `<groupid>`. If `<all>` is selected, all physical interfaces will be added to this protocol group. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default	none
Format	config protocol interface add <groupid> <slot.port/ all>

config protocol interface remove

This command removes the `<interface>` from this protocol-based VLAN group that is identified by this `<groupid>`. If `<all>` is selected, all ports will be removed from this protocol group.

Default	none
Format	config protocol interface remove <groupid> <slot.port/all>

show garp info

This command displays Generic Attributes Registration Protocol (GARP) information.

Format	show garp info
GMRP Admin Mode	This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

show garp interface

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	show garp interface <slot.port/all>
Interface	This displays the slot.port of the interface that this row in the table describes.
Join Timer	Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP

	participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	Specifies the period of time to wait after receiving an unregistered request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Port GMRP Mode	Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.
Port GVRP Mode	Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

config garp gmrp adminmode

This command enables or disables GARP Multicast Registration Protocol (GMRP) on the system. The default value is disable.

Format `config garp gmrp adminmode <enable/disable>`

config garp gmrp interface mode

This command enables or disables GARP Multicast Registration Protocol on a selected interface. The <slot.port> parameter identifies the interface on which to configure the mode. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a LAG, GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and LAG membership is removed from an interface that has GARP enabled.

Default `disable`
Format `config garp gmrp interface mode <slot.port/all> <enable/disable>`

config garp gvrp adminmode

This command enables or disables GVRP.

Default	disable
Format	config garp gvrp adminmode <enable disable>

config garp gvrp interface mode

This command enables or disables GVRP (GARP VLAN Registration Protocol) for a specific port. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Default	disable
Format	config garp gvrp interface mode <slot.port all> <enable disable>

config garp jointimer

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.

This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds)

Default	20 centiseconds (0.2 seconds)
Format	config garp jointimer <slot.port/all> <10-100>

config garp leavetimer

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service.time is 20 to 600 (centiseconds).

Note: This command has an effect only when GVRP is enabled.

Default	60 centiseconds (0.6 seconds)
Format	config garp leavetimer <slot.port/all> <20-600>

config garp leavealltimer

This command sets how frequently Leave All PDUs are generated per port. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds).

Note: This command has an effect only when GVRP is enabled.

Default	1000 centiseconds (10 seconds)
Format	config garp leavealltimer <slot.port/all> <200-6000>

show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

Format	show igmpsnooping
Admin Mode	This indicates whether or not IGMP Snooping is active on the switch.
Query Interval Time	This displays the IGMP Query Interval Time. This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured
Max Response Time	This displays the amount of time the switch will wait after sending a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Present Expiration Time	If a query is not received on an interface within this amount of time, the interface is removed from the list of interfaces with multicast routers attached. This value may be configured.
Interfaces Enabled for GMP Snooping	This is the list of interfaces on which IGMP Snooping is enabled.

The following status values are only displayed when IGMP Snooping is enabled.

Multicast Control Frame Count	This displays the number of multicast control frames that are processed by the CPU.
Data Frames Forwarded by the CPU	This displays the number of data frames that are forwarded by the CPU.

config igmpsnooping adminmode

This command enables or disables IGMP Snooping on the system. The default value is disable.

Format	config igmpsnooping adminmode <enable/disable>
---------------	---

config igmpsnooping groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP Maximum Response time value. The range is 1 to 3600 seconds.

Default	260 seconds
Format	config igmpsnooping groupmembershipinterval <1-3600>

config igmpsnooping maxresponse

This command sets the IGMP Maximum Response time on the system. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3600 seconds.

Default	10 seconds
Format	config igmpsnooping maxresponse <1-3600>

config igmpsnooping mcrtrexpiretime

This command sets the Multicast Router Present Expiration time on the system. This is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default	0
Format	config igmpsnooping mcrtrexpiretime <0-3600>

config igmpsnooping interface mode

This command enables or disables IGMP Snooping on a selected interface. The <slot.port/all> parameter identifies the interface on which to configure the mode. If an interface which has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a LAG, IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or LAG membership is removed from an interface that has IGMP Snooping enabled.

Default	disable
Format	config igmpsnooping interface mode <slot.port/all> <enable/disable>

show mfdb table

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional *all* parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format	show mfdb table [macaddr/all]
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mfdb gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

Format	show mfdb gmrp
---------------	-----------------------

Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format	show mfdb igmpsnooping
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format	show mfdb staticfiltering
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format	show mfdb stats
Total Entries	This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	This displays the current number of entries in the Multicast Forwarding Database table.

show mirroring

This command displays the Port Mirroring information for the system.

Format	show mirroring
Port Mirroring Mode	Indicates whether the Port Mirroring feature is enabled or disabled. The possible values are enable and disable.
Probe Port Slot.Port	Is the slot.port that is configured as the probe port. If this value has not been configured, 'Not Configured' will be displayed.
Mirrored Port Slot.Port	Is the slot.port that is configured as the mirrored port. If this value has not been configured, 'Not Configured' will be displayed.

config mirroring create

This command configures a probe port and a mirrored port for Port Mirroring. The first slot.port is the probe port and the second slot.port is the mirrored port. If this command is executed while port mirroring is enabled, it will have the effect of changing the probe and mirrored port values.

Format	config mirroring create <slot.port> <slot.port>
---------------	--

config mirroring delete

This command removes the port mirroring designation from both the probe port and the mirrored port and removes the probe port from all VLANs. The port must be manually re-added to any desired VLANs.

Format	config mirroring delete
---------------	--------------------------------

config mirroring mode

This command configures the Port Mirroring mode. The possible values are enable and disable. The default value is disable. The probe and mirrored ports must be configured before port mirroring can be enabled. If enabled, the probe port will mirror all traffic received and transmitted on the physical mirrored port. It is not necessary to disable port mirroring before modifying the probe and mirrored ports.

Default	disable
Format	config mirroring mode <enable disable>

show macfilter

This command displays the Static MAC Filtering information for all Static MAC Filters. If <all> is selected, all the Static MAC Filters in the system are displayed. If a macaddr is entered, a vlan must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN.

Format	show macfilter <macaddr vlan/all>
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	Indicates the source port filter set's slot and port(s).
Destination Port(s)	Indicates the destination port filter set's slot and port(s).

config macfilter create

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

The <vlan> parameter must identify a valid VLAN.

Up to 100 static MAC filters may be created.

Format `config macfilter create <macaddr> <vlan>`

config macfilter remove

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlan> parameter must identify a valid VLAN.

Format `config macfilter remove <macaddr> <vlan>`

config macfilter addsrc

This command adds the <slot.port> to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlan> parameter must identify a valid VLAN.

The `<slot.port>` parameter identifies the source port to be added to the source port filter set for the MAC filter.

If all is selected, all ports will be added to the source port filter set.

Format `config macfilter addsrc <macaddr> <vlan>`
 `<slot.port|all>`

config macfilter delsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlan> parameter must identify a valid VLAN.

The <slot.port> parameter identifies the source port to be removed from the source port filter set for the MAC filter.

If all is selected, all ports will be removed from the source port filter set.

Format	config macfilter delsrc <macaddr> <vlan> <slot.port all>
---------------	---

config macfilter adddest

This command adds the <slot.port> to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlan> parameter must identify a valid VLAN.

The <slot.port> parameter identifies the destination port to be added to the destination port filter set for the MAC filter.

If all is selected, all ports will be added to the destination port filter set.

Format	config macfilter adddest <macaddr> <vlan> <slot.port all>
---------------	--

config macfilter deldest

This command removes a port from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlan>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlan> parameter must identify a valid VLAN.

The <slot.port> parameter identifies the destination port to be removed from the destination port filter set for the MAC filter.

If all is selected, all ports will be removed from the destination port filter set.

Format	config macfilter deldest <macaddr> <vlan> <slot.port all>
---------------	--

Spanning Tree Commands

This section provides detailed explanation of the spanning tree commands. The commands are divided into two functional groups:

- Show commands display spanning tree settings, statistics, and other information.
- Config commands configure features and options of the switch. For every config command there is a show command that displays the config setting.

This section is organized by configuration type:

- System information and statistics commands
- Bridge and CIST commands
- MSTI commands
- Modified commands
- Obsolete commands

show spanningtree summary

This command displays spanning tree settings and parameters for the switch.

Format	show spanningtree summary
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
Configuration Name	TConfigured name.
Configuration Revision	
Level	Configured value.
Configuration Digest Key	Calculated value.
Configuration Format Selector	Configured value.
MST Instances	List of all multiple spanning tree instances configured on the switch.

config spanningtree adminmode

This command sets the spanningtree operational mode. While disabled, the spanningtree configuration is retained and can be changed, but it is not activated.

Default	disable
Format	config spaningtree adminmode <enable/disable>

config spanningtree forceversion

This command sets the Force Protocol Version parameter to a new value. The <version> can be one of the following:

- 802.1d - ST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1d functionality supported)
- 802.1w - RST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1w functionality supported)
- 802.1s - MST BPDUs are transmitted (IEEE 802.1s functionality supported)

Default 802.1s

Format **config spanningtree forceversion <802.1d/802.1w/802.1s>**

config spanningtree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The <name> is a string of at most 32 characters.

Default The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Format **config spanningtree configuration name <name>**

config spanningtree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The <revision> is a number in the range of 0 to 65535.

Default 0

Format **config spanningtree configuration revision <0-65535>**

show spanningtree port

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot.port> is the desired switch port.

Format **show spanningtree port <slot.port>**

Port mode Enabled or disabled.

Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RST BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

config spanningtree port migrationcheck

This command forces the specified port to transmit RST or MST BPDUs. The port <slot.port> is the desired switch port. To set the migration check for all ports with a single command, "all" can be specified. Note that the forceversion parameter for the switch must be set to 802.1w or 802.1s.

Default	disable
Format	config spanningtree port migrationcheck <slot.port/all> <enable/disable>

config spanningtree port mode

This command sets the Administrative Switch Port State to a new value for the specified port. The port <slot.port> is the desired switch port. To enable or disable all ports with a single command, "all" can be specified. Note that only 4095 ports can be enabled.

Default	disable
Format	config spanningtree port mode <slot.port/all> <enable/disable>

show spanningtree bridge

This command displays spanning tree settings for the bridge.

Format	show spanningtree bridge
Bridge Priority	Configured value.
Bridge Identifier	
Bridge Max Age	TConfigured value.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

config spanningtree bridge maxage

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The maxage <value> is in whole seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

Default	20
Format	config spanningtree bridge maxage <6-40>

config spanningtree bridge hellotime

This command sets the Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 10 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

Default	2
Format	config spanningtree bridge hellotime <1-10>

config spanningtree bridge forwarddelay

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forwarddelay <value> is in whole seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default	15
Format	config spanningtree bridge forwarddelay <4-30>

config spanningtree bridge priority

This command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority <value> is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

Default	32768
Format	config spanningtree bridge priority <0-61440>

show spanningtree cst detailed

This command displays spanning tree settings for the common and internal spanning tree.

Format	show spanningtree cst detailed
Bridge Priority	Configured value.
Bridge Identifier	
Time Since Topology Change	In seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Derived value.
Root Port Max Age	Derived value.
Root Port Bridge	
Forward Delay	Derived value.
Hello Time	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	
Regional Root Path Cost	
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanningtree cst port summary

This command displays the status of one or all ports within the common and internal spanning tree. The parameter <slot.port/all> indicates the desired switch port or all ports.

Format	show spanningtree cst port summary <slot.port/all>
MST Instance ID	CST
Slot.Port	The interface being displayed.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Link Status	The operational status of the link. Possible values are “Up” or “Down”.
Link Trap	The link trap configuration for the specified interface.

show spanningtree cst port detailed

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot.port> is the desired switch port

Format	show spanningtree cst port detailed <slot.port>
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Port Path Cost	The configured path cost for the specified interface.
Designated Root	Identifier of the designated root for this port within the CST.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Port Cost	The configured path cost for this port.

config spanningtree cst port pathcost

This command sets the Path Cost to a new value for the specified port in the common and internal spanning tree. The <slot.port> is the desired switch port. The pathcost <value> can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

Default	auto
Format	config spanningtree cst port pathcost <slot.port> <1-200000000/auto>

config spanningtree cst port priority

This command sets the Port Priority to a new value for use within the common and internal spanning tree. The <slot.port> is the desired switch port. The priority <value> is a number in the range of 0 to 240 in increments of 16.

Default	128
Format	config spanningtree cst port priority <slot.port> <0-240>

config spanningtree cst port edgeport

This command specifies if a port is an Edge Port within the common and internal spanning tree. This will allow the port to transition to Forwarding State without delay. The <slot.port> is the desired switch port. The edgeport <value> can either be "true" or "false".

Default	false
Format	config spanningtree cst port edgeport <slot.port> <true/false>

config spanningtree mst create

This command adds a multiple spanning tree instance to the switch. The instance <mstid> is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by managed switch software is 4.

Format	config spanningtree mst create <mstid>
---------------	---

config spanningtree mst delete

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	config spanningtree mst delete <mstid>
---------------	---

config spanningtree mst vlan add

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlan> corresponds to an existing VLAN ID.

Format `config spanningtree mst vlan add <mstid> <vlan>`

config spanningtree mst vlan remove

This command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlan> corresponds to an existing VLAN ID.

Format `config spanningtree mst vlan remove <mstid> <vlan>`

config spanningtree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The priority <value> is a number within a range of 0 to 61440 in increments of 4096.

Default	32768
---------	-------

Format `config spanningtree mst priority <mstid> <0-61440>`

config spanningtree mst port pathcost

This command sets the path cost for a specific port within a multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot.port> is the desired switch port. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

Default	auto
----------------	------

```
Format          config spanningtree mst port pathcost <mstid>
                  <slot.port> <1-200000000/auto>
```

config spanningtree mst port priority

This command sets the priority for a specific port within a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot.port> is the desired switch port. The priority <value> is a number in the range of 0 to 240 in increments of 16.

Default	128
Format	config spanningtree mst port priority <mstid> <slot.port> <0-240>

show spanningtree mst summary

This command displays summary information about all multiple spanning tree instances in the switch.

Format	show spanningtree mst summary
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID:	
Associated FIDs	List of forwarding database identifiers associated with this instance.
Associated VLANs	List of VLAN IDs associated with this instance.

show spanningtree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance ID.

Format	show spanningtree mst detailed <mstid>
MST Instance ID	
MST Bridge Priority	
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times the topology has changed for this multiple spanning tree instance.
Topology Change in Progress	Value of the Topology Change parameter for the multiple spanning tree instance.
Designated Root	Identifier of the Regional Root for this multiple spanning tree instance.
Root Path Cost	Path Cost to the Designated Root for this multiple spanning tree instance.
Root Port Identifier	Port to access the Designated Root for this multiple spanning tree instance.
Associated FIDs	List of forwarding database identifiers associated with this instance.
Associated VLANs	List of VLAN IDs associated with this instance.

show spanningtree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <mstid> indicates a particular MST instance. The parameter <slot.port/all> indicates the desired switch port or all ports.

Format	show spanningtree mst port summary <mstid> <slot.port/all>
MST Instance ID	The MST instance associated with this port.
Slot.Port	The interface being displayed.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Link Status	The operational status of the link. Possible values are “Up” or “Down”.
Link Trap	The link trap configuration for the specified interface.

show spanningtree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot.port> is the desired switch port.

Format	show spanningtree mst port detailed <mstid> <slot.port>
MST Instance ID	
Port Identifier	
Port Priority	
Port Forwarding State	Current spanning tree state of this port.
Port Role	
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.

show spanningtree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <vlan> corresponds to an existing VLAN ID.

Format	show spanningtree vlan <vlan>
---------------	--

VLAN Identifier

Associated Instance

Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree.

User Account Management Commands

These commands manage user accounts.

show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format

User Name

show users

The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, admin and guest.

Access Mode

Shows whether the operator is able to change parameters on the switch(Read/Write) or is only able to view them(Read Only). As a factory default, admin has Read/Write access and guest has Read Only access. There can only be one Read/Write user and up to 5 Read Only users.

SNMPv3AccessMode

This field displays the SNMPv3 Access Mode. If the value is set to **ReadWrite**, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to **ReadOnly**, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3Authentication

This field displays the authentication protocol to be used for the specified login user.

SNMPv3Encryption

This field displays the encryption protocol to be used for the specified login user.

config users add

This command adds a new user (account) if space permits. The account <name> is up to eight alphanumeric characters. The <name> is not case-sensitive.

Six user names can be defined.

Format

config users add <name>

config users passwd

This command changes the password of an existing operator. The password is up to eight alphanumeric characters. The name and password are not case-sensitive.

When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

Default	Blank (indicating no password)
Format	config users passwd <user>

config users delete

This command removes an operator.

Format	config users delete <name>
Note:	The admin user account cannot be deleted.

config users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are **none**, **md5** or **sha**. If **md5** or **sha** are specified, the user login password will be used as the snmpv3 authentication password. The **<user>** is the login user name for which the specified authentication protocol will be used.

Default	no authentication
Format	config users snmpv3 authentication <user> <none/md5/sha>

config users snmpv3 encryption

This command specifies the encryption protocol and key to be used for the specified login user. The valid encryption protocols are **none** or **des**. The **des** protocol requires a **key**, which can be specified on the command line. The **key** may be up to 16 characters long. If the **des** protocol is specified but a key is not provided, the user will be prompted for the key. If **none** is specified, a key must not be provided. The **<user>** is the login user name for which the specified encryption protocol will be used.

Default	no encryption
Format	config users snmpv3 encryption <user> <none/des [key]>

config users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are **readonly** or **readwrite**. The **<user>** is the login user name for which the specified access mode will apply.

Default	readwrite for admin user; readonly for all other users
Format	config users snmpv3 accessmode <user> <readonly/readwrite>

show loginsession

This command displays current telnet and serial port connections to the switch.

Format	show loginsession
ID	Login Session ID.
User Name	The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, admin and guest.
Connection From	IP address of the telnet client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.

config loginsession close

This command closes a telnet session.

Format	config loginsession close <sessionID/all>
---------------	--

Security Commands

This section describes commands used for configuring security settings for login users and port users.

This command permanently saves configuration changes to Non-Volatile Random Access Memory (NVRAM).

Format	save config
---------------	--------------------

config radius maxretransmit

This command sets the maximum number of times a request packet is retransmitted when no response is received from the RADIUS server. The maxretransmit value is an integer in the range of 1 and 15.

Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

Default	4
Format	config radius maxretransmit <1-15>

config radius timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the radius server if no response is received. The timeout value is an integer in the range of 1 and 30.

Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

Default	5
Format	config radius timeout <1-30>

config radius accounting mode

This command enables or disables the RADIUS accounting function.

Default	disable
----------------	---------

Format `config radius accounting mode <enable/disable>`

config radius accounting server add

This command configures the IP address to use for the accounting server. Only a single accounting server can be configured. If an accounting server is currently configured it must be removed using the 'config radius accounting server remove' command before the add command will succeed.

Format `config radius accounting server add <ipaddr>`

config radius accounting server port

This command configures the UDP port to use for the accounting server. The IP address specified must match that of the previously configured accounting server. If a port is already configured for the accounting server, the new port will replace the previously configured value. The port must be a value in the range of 0 and 65535.

Default 1813

Format `config radius accounting server port <ipaddr> <0-65535>`

config radius accounting server remove

This command removes a configured accounting server. The IP address specified must match that of the previously configured accounting server. Since only a single accounting server is supported, issuing this command will cause future accounting attempts to fail.

Format `config radius accounting server remove <ipaddr>`

config radius accounting server secret

This command configures the shared secret between the RADIUS client and the RADIUS accounting server. The IP address specified must match that of the previously configured accounting server. When this command is issued, the secret will be prompted. The secret must be an alphanumeric value of 20 characters or less.

Format `config radius accounting server secret <ipaddr>`

config radius server add

This command configures the IP address to use to connect to a RADIUS server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers has been reached, this command will fail until one of the servers is removed using the ‘config radius server remove’ command. Once a server is added, it is referenced in later ‘config radius server’ commands using the configured IP address.

Format config radius server add <ipaddr>

```
config radius server port
```

This command configures the UDP port number to use to connect to the specified RADIUS server. The IP address specified must match that of a previously configured RADIUS server. The port number must be in the range of 0 and 65535.

Default	1812
---------	------

Format `config radius server port <ipaddr> <0-65535>`

config radius server remove

This command removes the configured RADIUS server. The specified IP address must match that of a previously configured RADIUS server. When a server is removed all configuration for the server is erased including the shared secret. If the removed server was the primary server, one of the remaining configured servers will be used as the RADIUS server for future RADIUS requests.

Format `config radius server remove <ipaddr>`

config radius server secret

This command configures on the client the shared secret between the RADIUS client and the RADIUS server. Each configured server requires a secret to be configured. The server is specified by the IP address. When this command is issued, the secret will be prompted. The secret must be an alphanumeric value of 20 characters or less.

Format `config radius server secret <ipaddr>`

config radius server primary

This command specifies which configured server should be the primary server for this RADIUS client. The primary is the server that is used by default for handling RADIUS requests. The remaining configured servers are used only if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one server can be configured as the primary server. If a primary server is currently configured and this command is issued, the server specified by the IP address used in this command will become the new primary server. The IP address specified must match that of a configured server.

Format `config radius server primary <ipaddr>`

config radius server msgauth

This command enables or disables the message authenticator attribute for the specified RADIUS server. Enabling the message authenticator attribute provides additional security in the connection between the RADIUS client and the RADIUS server. Some RADIUS servers require enabling the message authenticator attribute for authentication requests from the RADIUS client to be accepted. The IP address specified must match that of a configured server.

Format `config radius server msgauth <ipaddr> <enable/disable>`

show radius summary

This command displays the following RADIUS configuration items for the switch.

Format	show radius summary
Current Server IP address	The IP address of the server currently used for authentication.
Number of Configured Servers	The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.
Max Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Timeout Duration	The configured timeout value, in seconds, for request retransmissions.
Accounting Mode	The configured value for RADIUS accounting mode indicating if accounting is currently enabled.

show radius server summary

This command displays the configured RADIUS servers.

Format `show radius server summary`

Current	Indicates the configured server currently in use for authentication.
IP address	The configured IP address of the authentication server.
Port	The port in use by this server.
Type	Primary or Secondary.
Secret Configured	Yes or No.

show radius server stats

This command displays the statistics for a configured RADIUS server. The IP address specified must match the IP address of a configured RADIUS server.

Format	show radius server stats <ipaddr>
Server IP address	
Round Trip Time	The time interval, in seconds, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

show radius accounting summary

This command displays the configured accounting mode and accounting server.

Format	show radius accounting summary
Mode	Enabled or Disabled.
IP address	The configured IP address of the accounting server.
Port	The port in use by the accounting server.
Secret Configured	Yes or No.

show radius accounting stats

This command displays the statistics for the accounting server. The IP address specified must match that of a configured accounting server.

Format	show radius accounting stats <ipaddr>
Accounting Server IP address	
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server
Accounting Requests	The number of RADIUS Accounting-Request packets sent not including retransmissions.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

show radius stats

This command displays the RADIUS statistics that are not related to a specific server or to the accounting server.

Format	show radius stats
Invalid Server Addresses	The number of RADIUS Access-Response packets received from unknown addresses.

clear radius stats

This command clears all RADIUS statistics.

Format	clear radius stats
---------------	--------------------

config dot1x adminmode

This command enables or disables authentication support on the switch. The default value is disable. While disabled, the dot1x configuration is retained and can be changed, but it is not activated.

Default	disable
Format	config dot1x adminmode <enable/disable>

config dot1x port initialize

This command begins the initialization sequence on the specified port. This command is only valid if dot1x is enabled and the control mode for the specified port is 'auto'.

Format	config dot1x port initialize <slot.port>
---------------	--

config dot1x port reauthenticate

This command begins the reauthentication sequence on the specified port. This command is only valid if dot1x is enabled and the control mode for the specified port is 'auto'.

Format	config dot1x port reauthenticate <slot.port>
---------------	--

config dot1x port controldir

This command configures the control direction for the specified port or ports. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames).

Default	both
Format	config dot1x port controldir <slot.port/all> <both/in>

config dot1x port controlmode

This command sets the authentication mode to be used on the specified port or ports. The control mode may be one of the following:

forceunauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized

forceauthorized: The authenticator PAE unconditionally sets the controlled port to authorized.

auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

Default	auto
Format	config dot1x port controlmode <slot.port/all> <forceunauthorized/forceauthorized/auto>

config dot1x port quietperiod

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a value in the range of 0 and 65535.

Default	60
Format	config dot1x port quietperiod <slot.port> <0-65535>

config dot1x port transmitperiod

This command sets the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period must be a value in the range of 1 and 65535.

Default	30
Format	config dot1x port transmitperiod <slot.port> <1-65535>

config dot1x port supptimeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supplicant timeout must be a value in the range of 1 and 65535.

Default	30
Format	config dot1x port supptimeout<slot.port> <1-65535>

config dot1x port servertimeout

This command sets the value, in seconds, of the timer used by the authenticator on this port to timeout the authentication server. The server timeout must be a value in the range of 1 and 65535.

Default	30
Format	config dot1x port servertimeout <slot.port> <1-65535>

config dot1x port maxrequests

This command sets the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The max requests value must be in the range of 1 and 10.

Default	2
Format	config dot1x port maxrequests <slot.port> <1-10>

config dot1x port reauthperiod

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthperiod must be a value in the range of 1 and 65535.

Default	3600
Format	config dot1x port reauthperiod <slot.port> <1-65535>

config dot1x port reauthenabled

This command enables or disables reauthentication of the supplicant for the specified port. The reauthenabled value must be 'true' or 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

Default	false
Format	config dot1x port reauthenabled <slot.port> <true/false>

show dot1x summary

This command displays a summary of the global dot1x configuration.

Format	show dot1x summary
Administrative mode	Indicates if authentication control is enabled on the switch. Possible values are Enabled and Disabled.

show dot1x port summary

This command displays a summary of the dot1x configuration for a specified port or for all ports.

Format	show dot1x port summary <slot.port/all>
Port	The interface whose configuration is displayed in this row.
Control Mode	The configured control mode for this port. Possible values are ForceUnauthorized, ForceAuthorized, or Auto.
Operating Control Mode	The control mode under which this port is operating. Possible values are ForceUnauthorized, ForceAuthorized, or Auto.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are True or False.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.

show dot1x port detailed

This command displays the details of the dot1x configuration for a specified port.

Format	show dot1x port detailed <slot.port>
Port	The interface whose configuration is displayed.

Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are True or False.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	Indicates the control direction for the specified port or ports. Possible values are both or in.

show dot1x port stats

This command displays the dot1x statistics for a specified port.

Format	show dot1x port stats <slot.port>
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

clear dot1x port stats

This command resets the dot1x statistics for the specified port or for all ports.

Format	clear dot1x port stats <slot,port/all>
---------------	---

config authentication login create

This command creates an authentication login list. The **<listname>** is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method. Authentication methods can be changed using the ‘config authentication login set’ command.

Default	None
Format	config authentication login create <listname>

config authentication login delete

This command deletes the specified authentication login list. The attempt to delete will fail if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the nonconfigured user for any component
- The login list is the default login list included with the default configuration and was not created using 'config authentication login create'. The default login list cannot be deleted.

Format	config authentication login delete <listname>
---------------	--

config authentication login set

This command sets an ordered list of methods in the authentication login list. The maximum number of authentication login methods is three. The possible method values are **local**, **radius**, and **reject**.

The value of **local** indicates that the user's locally stored ID and password are used for authentication. The value of **radius** indicates that the user's ID and password will be authenticated using the RADIUS server. The value of **reject** indicates that the user is never authenticated.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

Note that the default login list included with the default configuration can not be changed.

Default	None
Format	config authentication login set <listname> <local/radius/reject> [local/radius/reject] [local/radius/reject]

config dot1x defaultlogin

This command assigns the authentication login list to use for nonconfigured users for 802.1x port security. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format **config dot1x defaultlogin <listname>**

config dot1x login

This command assigns the specified authentication login list to the specified user for port security. The <user> must be a configured <user> and the <listname> must be a configured login list.

Format **config dot1x login <user> <listname>**

config dot1x port users add

This command adds the specified user to the list of users with access to the specified port. The <user> must be a configured <user> and the <port> must be a valid port. By default, a user is given access to all ports.

Default Access to all ports
Format **config dot1x port users add <user> <slot.port/all>**

config dot1x port users remove

This command removes the specified user from the list of users with access to the specified port.

Format **config dot1x port users remove <user> <slot.port/all>**

config users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format **config users defaultlogin <listname>**

config users login

This command assigns the specified authentication login list to the specified user for system login. The **<user>** must be a configured **<user>** and the **<listname>** must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete. Refer to the discussion of maximum delay in the ‘config radius maxretransmit’ and ‘config radius timeout’ commands.

Note that the login list associated with the ‘admin’ user can not be changed to prevent accidental lockout from the switch.

Format	config users login <user> <listname>
---------------	---

show authentication login info

This command displays the ordered authentication methods for all authentication login lists.

Format	show authentication login info
Authentication Login List	This displays the authentication login listname.
Method 1	This displays the first method in the specified authentication login list, if any.
Method 2	This displays the second method in the specified authentication login list, if any.
Method 3	This displays the third method in the specified authentication login list, if any.

show authentication login users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format	show authentication login users <listname>
User	This field displays the user assigned to the specified authentication login list.
Component	This field displays the component (User or 802.1x) for which the authentication login list is assigned.

show dot1x port users

This command displays 802.1x port security user information for locally configured users.

Format	show dot1x port users <slot.port>
---------------	--

User	This field displays the users configured locally to have access to the specified port.
-------------	--

show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format	show users authentication
User	This field lists every user that has an authentication login list assigned.
System Login	This field displays the authentication login list assigned to the user for system login.
802.1x Port Security	This field displays the authentication login list assigned to the user for 802.1x port security.

System Utilities

This section describes system utilities.

save config

This command permanently saves configuration changes to Non-Volatile Random Access Memory (NVRAM).

Format	save config
---------------	--------------------

logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out. See “save config” on page 74.

Format	logout
---------------	---------------

transfer upload mode

This command specifies whether XMODEM or TFTP mode is used when uploading from the switch.

Default	xmodem. This is valid only when the transfer is initiated by the serial EIA 232 port.
----------------	--

Format transfer upload mode <xmodem|tftp>

transfer upload serverip

This command sets the IP address of the server on which the file is located.

Note: This command is valid only when the transfer mode is TFTP. See “transfer upload mode”.

Default	0.0.0.0
---------	---------

Format transfer upload serverip <ipaddr>

transfer upload path

This command sets the directory path used to upload the file. The switch “remembers” the last file path used.

Note: This command is valid only when the transfer mode is TFTP. See “transfer upload mode”.

GSM7224 Layer 2 Managed Switch software supports the TFTP client. The TFTP client path statement requirement is sever dependent. A path statement is generally required to set up the TFTP client; however, the client path may remain blank.

See the example of the path setup.

TFTP Upload Example: The TFTP upload example details three scenarios for TFTP client to server file transfer.

In the example, the operator will upload the config.bin file from the switch to the location c:\tftp\ on the server. The different scenarios are detailed below:

Table 3. TFTP Upload Example.

TFTP Server path	TFTP Client path
c:\tftp\	blank
c:\	tftp\
c:	\tftp\

GSM7224 Layer 2 Managed Switch software provides two methods to clear the directory path statement.

- The **clear config** command will remove the directory path statement.
- The web browser clear command will remove the directory path statement.

Default	Blank
	

Format `transfer upload path <path>`

transfer upload filename

This command sets the name for the file that is uploaded from the switch. The switch “remembers” the last file name used.

Append the file path to the file name if the string is less than 31 characters. Otherwise, use the “transfer upload path” command, and the File Name will be appended to the File Path.

Note: This command is valid only when the Transfer Mode is TFTP. See “transfer upload mode”.

Default	Blank
Format	transfer upload filename <name>

transfer upload datatype

This command sets the type of file to upload from the switch.

Format	transfer upload datatype <config errorlog msglog traplog>
---------------	--

The datatype is one of the following:

config	Configuration file.
errorlog	Error log.
msglog	Message log.
traplog	Trap log (the default).

transfer upload start

This command starts an upload transfer after displaying current settings and upon confirmation.

Format	transfer upload start
---------------	------------------------------

transfer download mode

This command specifies whether XMODEM or TFTP mode is used when uploading from the switch.

Default	xmodem. This is valid only when the transfer is initiated by the serial EIA 232 port.
Format	transfer download mode <xmodem tftp>

transfer download serverip

This command configures the IP address of the server on which the file is located.

Note: This command is valid only when the transfer mode is TFTP. See “transfer download mode” .

Default	0.0.0.0
Format	transfer download serverip <ipAddr>

transfer download path

This command sets the directory path used to download the file. The switch “remembers” the last file path used.

Note: This command is valid only when the Transfer Mode is TFTP. See “transfer download mode” on page 76. Details of the TFTP path are explained under the command **transfer upload path <path>**.

Default	Blank
Format	transfer download path <path>

transfer download filename

This command sets the name for the file that is downloaded to the switch. The switch “remembers” the last file name used.

Append the file path to the file name if the string is less than 31 characters. Otherwise, use the transfer download path command, and the File Name will be appended to the File Path as is.

Note: This command is valid only when the Transfer Mode is TFTP. See “transfer download mode” on page 76.

Default	Blank
Format	transfer download filename <name>

transfer download datatype

This command sets the type of file to download to the switch.

Default	code
Format	transfer download datatype <code config>

transfer download start

This command starts a download transfer after displaying current settings and upon confirmation.

Format **transfer download start**

clear transfer

This command resets the file transfer configured values to the factory defaults.

Format **clear transfer**

clear config

This command resets the configuration to the factory defaults without powering off the switch. The switch is automatically reset when this command is processed. You are prompted to confirm that the reset should proceed.

Format **clear config**

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format **clear pass**

clear traplog

This command clears the trap log.

Format **clear traplog**

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format **clear vlan**

clear lag

This command clears all LAGs.

Format **clear lag**

clear stats port

This command clears the stats for a specified <slot.port>

Format **clear stats port <slot.port>**

clear stats switch

This command clears the stats for the switch.

Format **clear stats switch**

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

Format **clear igmpsnooping**

reset system

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format **reset system**

ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection (as described in the *FASTPATH^{mp} 2402/4802 Hardware User Guide*). The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends, three pings to the target station.

Format

ping <ipaddr>

Chapter 8

Differentiated Services

This chapter contains the Command Line Interface (CLI) commands used for the QOS Differentiated Services (DiffServ) package.

The GSM7224 Layer 2 Managed Switch provides a simplified interface for enabling DiffServ support. A single command is used to enable and disable this function:

config diffserv adminmode <enable/disable>

When enabled, the device inspects the DSCP of each packet to determine whether the packet should receive preferential treatment. That is, the class of service given to the packet is determined by the DSCP. When disabled, the DSCP is not used for determining the class of service given to the packet.

The current status of the DiffServ function can be determined with the following command:

show diffserv info

Appendix A

Cabling Guidelines

This appendix provides specifications for cables used with a NETGEAR GSM7224 Layer 2 Managed Switch.

Fast Ethernet Cable Guidelines

Fast Ethernet uses UTP cable, as specified in the IEEE 802.3u standard for 100BASE-TX. The specification requires Category 5 UTP cable consisting of either two-pair or four-pair twisted insulated copper conductors bound in a single plastic sheath. Category 5 cable is certified up to 100 MHz bandwidth. 100BASE-TX operation uses one pair of wires for transmission and the other pair for receiving and for collision detection.

When installing Category 5 UTP cabling, use the following guidelines to ensure that your cables perform to the following specifications:

Certification

Make sure that your Category 5 UTP cable has completed the Underwriters' Laboratories (UL) or Electronic Testing Laboratories (ETL) certification process.

Termination method

To minimize cross-talk noise, maintain the twist ratio of the cable up to the point of termination; untwist at any RJ-45 plug or patch panel should not exceed 0.5 inch (1.5 cm).

Category 5 Cable

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

Category 5 Cable Specifications

Ensure that the fiber cable is crossed over to guarantee link.

Table F-1 lists the electrical requirements of Category 5 UTP cable.

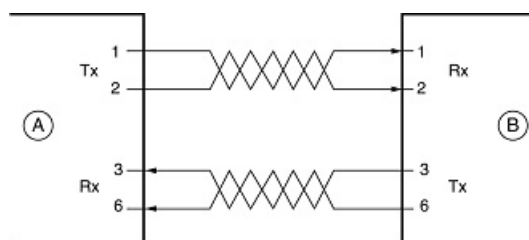
Table 8-1. Electrical Requirements of Category 5 Cable

SPECIFICATIONS	CATEGORY 5 CABLE REQUIREMENTS
Number of pairs	Four
Impedance	100 $\pm$ 15%
Mutual capacitance at 1 KHz	5.6 nF per 100 m
Maximum attenuation (dB per 100 m, at 20° C)	at 4 MHz: 8.2 at 31 MHz: 11.7 at 100 MHz: 22.0
NEXT loss (dB minimum)	at 16 MHz: 44 at 31 MHz: 39 at 100 MHz: 32

Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

Figure 8-1 illustrates straight-through twisted pair cable.



Key:

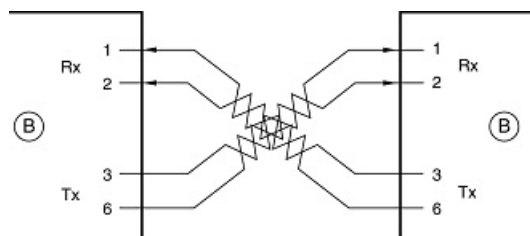
A = UPLINK OR MDI PORT (as on a PC)

B = Normal or MDI-X port (as on a hub or switch)

1, 2, 3, 6 = Pin numbers

Figure 8-1: Straight-Through Twisted-Pair Cable

Figure 8-2 illustrates crossover twisted pair cable.



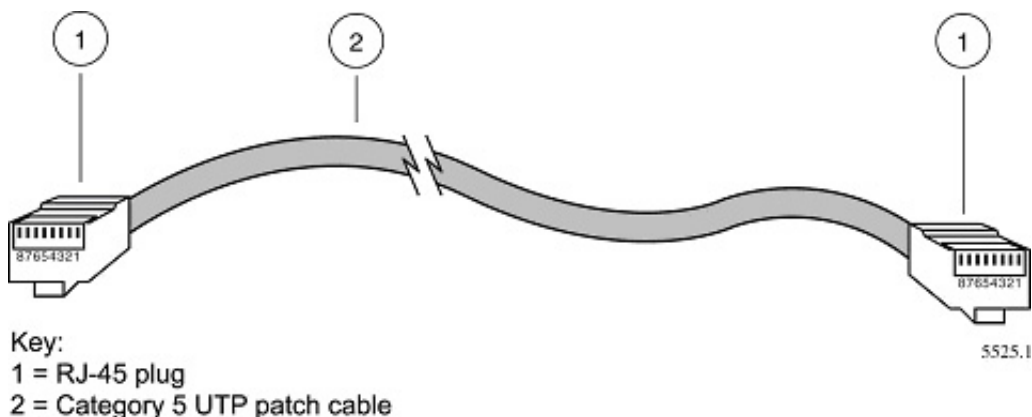
Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure 8-2: Crossover Twisted-Pair Cable

Patch Panels and Cables

If you are using patch panels, make sure that they meet the 100BASE-TX requirements. Use Category 5 UTP cable for all patch cables and work area cables to ensure that your UTP patch cable rating meets or exceeds the distribution cable rating.

To wire patch panels, you need two Category 5 UTP cables with an RJ-45 plug at each end, as shown here.



Key:
1 = RJ-45 plug
2 = Category 5 UTP patch cable

Figure 8-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Using 1000BASE-T Gigabit Ethernet over Category 5 Cable

When using the new 1000BASE-T standard, the limitations of cable installations and the steps necessary to ensure optimum performance must be considered. The most important components in your cabling system are patch panel connections, twists of the pairs at connector transition points, the jacket around the twisted-pair cable, bundling of multiple pairs on horizontal runs and punch down blocks. All of these factors affect the performance of 1000BASE-T technology if not correctly implemented. The following sections are designed to act as a guide to correct cabling for 1000BASE-T.

Cabling

The 1000BASE-T product is designed to operate over Category 5 cabling. To further enhance the operation, the cabling standards have been amended. The latest standard is Category 5e, which defines a higher level of link performance than is available with Category 5 cable.

If installing new cable, we recommend using Category 5e cable, since it costs about the same as Category 5 cable. If using the existing cable, be sure to have the cable plant tested by a professional who can verify that it meets or exceeds either ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications.

Length

The maximum distance limitation between two pieces of equipment is 100 m, as per the original Ethernet specification. The end-to-end link is called the “channel.”

TSB-67 defines the “Basic Link” which is the portion of the link that is part of the building infrastructure. This excludes patch and equipment cords. The maximum basic link length is 295 feet (90 m).

Return Loss

Return loss measures the amount of reflected signal energy resulting from impedance changes in the cabling link. The nature of 1000BASE-T renders this measurement very important; if too much energy is reflected back on to the receiver, the device does not perform optimally.

Unlike 10BASE-T and 100BASE-TX, which use only two of the four pairs of wires within the Category 5, 1000BASE-T uses all four pairs of the twisted pair. Make sure all wires are tested — this is important.

Factors that affect the return loss are:

The number of transition points, as there is a connection via an RJ-45 to another connector, a patch panel, or device at each transition point.

Removing the jacket that surrounds the four pairs of twisted cable. It is highly recommended that, when RJ-45 connections are made, this is minimized to 1-1/4 inch (32 mm).

Untwisting any pair of the twisted-pair cabling. It is important that any untwisting be minimized to 3/8 inch (10 mm) for RJ-45 connections.

Cabling or bundling of multiple Category 5 cables. This is regulated by ANSI/EIA/TIA-568A-3. If not correctly implemented, this can adversely affect all cabling parameters.

Near End Cross Talk (NEXT)

This is a measure of the signal coupling from one wire to another, within a cable assembly, or among cables within a bundle. NEXT measures the amount of cross-talk disturbance energy that is detected at the near end of the link — the end where the transmitter is located. NEXT measures the amount of energy that is “returned” to the sender end. The factors that affect NEXT and cross talk are exactly the same as outlined in the Return Loss section. The cross-talk performance is directly related to the quality of the cable installation.

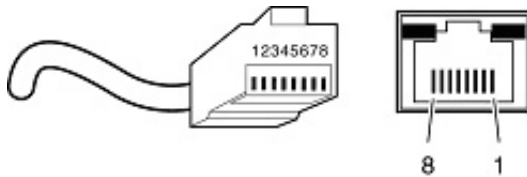
Patch Cables

When installing your equipment, replace old patch panel cables that do not meet Category 5e specifications. As pointed out in the NEXT section, this near end piece of cable is critical for successful operation.

RJ-45 Plug and RJ-45 Connectors

In a Fast Ethernet network, it is important that all 100BASE-T certified Category 5 cabling use RJ-45 plugs. The RJ-45 plug accepts 4-pair UTP or shielded twisted-pair (STP) 100-ohm cable and connects into the RJ-45 connector. The RJ-45 connector is used to connect stations, hubs, and switches through UTP cable; it supports 10 Mbps, 100 Mbps, or 1000 Mbps data transmission.

Figure 8-4 shows the RJ-45 plug and RJ-45 connector.



Key:
1 to 8 = pin numbers

Figure 8-4: RJ-45 Plug and RJ-45 Connector with Built-in LEDs

Table 8-1 lists the pin assignments for the 10/100 Mbps RJ-45 plug and the RJ-45 connector.

Table 8-1. 10/100 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

PIN	NORMAL ASSIGNMENT ON PORTS 1 TO 8	UPLINK ASSIGNMENT ON PORT 8
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data –	Output Transmit Data –
3	Output Transmit Data +	Input Receive Data +
6	Output Transmit Data –	Input Receive Data –
4, 5, 7, 8	Internal termination, not used for data transmission	

Table E-2 lists the pin assignments for the 100/1000 Mbps RJ-45 plug and the RJ-45 connector.

Table 8-2. 100/1000 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

PIN	CHANNEL	DESCRIPTION
1 2	A	Rx/Tx Data + Rx/Tx Data
3 6	B	Rx/Tx Data + Rx/Tx Data
4 5	C	Rx/Tx Data + Rx/Tx Data
7 8	D	Rx/Tx Data + Rx/Tx Data

Conclusion

For optimum performance of your 1000BASE-T product, it is important to fully qualify your cable installation and ensure it meets or exceeds ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications. Install Category 5e cable where possible, including patch panel cables. Minimize transition points, jacket removal, and untwist lengths. Bundling of cables must be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.

Appendix B

Glossary

Use the list below to find definitions for technical terms used in this manual.

Numeric

802.1D

The IEEE designator for Spanning Tree Protocol (STP). STP, a link management protocol, is part of the 802.1D standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing endless loops in a network. An endless loop is created by multiple active paths between stations where there are alternate routes between hosts. To establish path redundancy, STP creates a logical tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

802.1P

The IEEE protocol designator for Local Area Network (LAN). This Layer 2 network standard improves support of time critical traffic, and limits the extent of high bandwidth multicast traffic within a bridged LAN. To do this, 802.1P defines a methodology for introducing traffic class priorities. The 802.1P standard allows priority to be defined in all 802 MAC protocols (Ethernet, Token Bus, Token Ring), as well as in FDDI. For protocols (such as Ethernet) that do not contain a priority field, 802.1P specifies a method for indicating frame priority based on the new fields defined in the 802.1Q (VLAN) standard.

802.1Q VLAN

The IEEE protocol designator for Virtual Local Area Network (VLAN). This standard provides VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame to allow eight priority levels (QoS) and to identify up to 4096 VLANs. See “VLAN” on page 17 for more information.

10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-FX

The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.

100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

1000BASE-SX

The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.

1000BASE-T

The IEEE specification for 1000 Mbps Gigabit Ethernet over Category 5 twisted-pair cable.
gain access.

A

Aging

When an entry for a node is added to the lookup table of a switch, it is given a timestamp. Each time a packet is received from a node, the timestamp is updated. The switch has a user-configurable timer that erases the entry after a certain length of time with no activity from that node.

Auto-negotiation

A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

AVL tree

Binary tree having the property that for any node in the tree, the difference in height between the left and right subtrees of that node is no more than 1.

B

BPDU

See “Bridge Protocol Data Unit” on page 3.

Bandwidth

The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (1 Gbps) for Gigabit Ethernet.

Baud

The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

BootP

See “Bootstrap Protocol” on page 3.

Bootstrap Protocol

An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BootP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.

Bridge Protocol Data Unit

BPDUs are the IEEE 802.1D MAC Bridge Management protocol that is the standard implementation of STP (Spanning Tree Protocol). It uses the STP algorithm to insure that physical loops in the network topology do not result in logical looping of network traffic. Using one bridge configured as root for reference, the BPDU switches one of two bridges forming a network loop into standby mode, so that only one side of a potential loop passes traffic. By examining frequent 802.1d configuration updates, a bridge in the standby mode can switch automatically into the forward mode if the other bridge forming the loop fails.

Broadcast

A packet sent to all devices on a network.

Broadcast storm

Multiple simultaneous broadcasts that typically absorb all the available network bandwidth and can cause a network to fail. Broadcast storms can be due to faulty network devices or network loops.

C

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).

This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Checksum

A simple error-detection scheme in which each transmitted message is identified with a numerical value based on the number of set bits in the message. The receiving station then applies a formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been corrupted.

CLI

See “Command Line Interface” on page 4.

Collision

A term used to describe two colliding packets in an Ethernet network. Collisions are a part of normal Ethernet operation, but a sudden prolonged increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic.

Command Line Interface

CLI is a line-item interface for configuring systems. (In the case of LVL7, it is one of the user interfaces they have programmed for allowing programmers to configure their system).

D

DHCP

See “Dynamic Host Configuration Protocol” on page 5.

Differentiated Services

Diffserv is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1P tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. Differentiated Services and the Class of Service approach provide a way to control traffic that is both more flexible and more scalability than the Quality of Service approach.

Diffserv

See “Differentiated Services” on page 4.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to

198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DVMRP

See “DNS” on page 4.

Dynamic Host Configuration Protocol

DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.

EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

EEPROM

See “Electronically Erasable Programmable Read Only Memory” on page 5.

Electronically Erasable Programmable Read Only Memory

EEPROM is also known as Flash memory. This is re-programmable memory.

Endstation

A computer, printer, or server that is connected to a network.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

F

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Fault isolation

A technique for identifying and alerting administrators about connections (such as those associated with switch ports) that are experiencing congestion or failure, or exceeding an administrator-defined threshold.

Fast STP

A high-performance Spanning Tree Protocol. See “STP” on page 16 for more information.

Filtering

The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.

Flash Memory

See “EEPROM” on page 5.

Flow Control

The process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it. There are many flow control mechanisms. One of the most common flow control protocols for asynchronous communication is called xon-xoff. In this case, the receiving device sends an “xoff” message to the sending device when its buffer is full. The sending device then stops sending data. When the receiving device is ready to receive more data, it sends an “xon” signal.

Forwarding

When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Full-duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

G

GARP

See “Generic Attribute Registration Protocol” on page 7.

GARP Information Propagation

GIP is the propagation of information between GARP participants for the same application in a bridge is carried out by a GIP component.

GARP Multicast Registration Protocol

GMRP provides a mechanism that allows Bridges and end stations to dynamically register (and subsequently, de-register) Group membership information with the MAC Bridges attached to the same LAN segment, and for that information to be disseminated across all Bridges in the Bridged LAN that support Extended Filtering Services. The operation of GMRP relies upon the services provided by the GARP.

GARP VLAN Registration Protocol

GVRP allows workstations to request admission to a particular VLAN for multicast purposes.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

GE

See “Gigabit Ethernet” on page 7.

Generic Attribute Registration Protocol

GARP provides a generic attribute dissemination capability that is used by participants in GARP Applications (called GARP Participants) to register and de-register attribute values with other GARP Participants within a Bridged LAN. The definition of the attribute types, the values that they can carry, and the semantics that are associated with those values when registered are specific to the operation of the GARP Application concerned.

Gigabit Ethernet

An Ethernet system that is designed to operate at 1000 Mbps (1 Gbps).

GIP

See “GARP Information Propagation” on page 7.

GMRP

See “GARP Multicast Registration Protocol” on page 7.

GVD

GARP VLAN Database.

GVRP

See “GARP VLAN Registration Protocol” on page 7.

H

Half-duplex

A system that allows packets to be transmitted and received, but not at the same time. Contrast with full-duplex.

I

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IGMP

See “Internet Group Management Protocol” on page 8.

IGMP Snooping

A series of operations performed by intermediate systems to add logic to the network to optimize the flow of multicast traffic; these intermediate systems (such as Layer 2 switches) listen for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic. See “Internet Group Management Protocol” on page 8 for more information.

Internet Group Management Protocol

IGMP is the standard for IP Multicasting on the Internet. IGMP is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group. All hosts conforming to Level 2 of the IP Multicasting specification require IGMP.

IP

See “Internet Protocol” on page 9.

IP Multicasting

Sending out data to distributed servers on the MBone (Multicast Backbone). For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

Internet Protocol

The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

L

LAN

See "Local Area Network" on page 10.

Learning

The bridge examines the Layer 2 source addresses of every frame on the attached networks (called listening) and then maintains a table, or cache, of which MAC addresses are attached to each of its ports.

Load balancing

The ability to distribute traffic across various ports of a device, such as a switch, to provide efficient, optimized traffic throughout the network.

Local Area Network

A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

Loop

An event that occurs when two network devices are connected by more than one path, thereby causing packets to repeatedly cycle around the network and not reach their destination.

M

MAC

(1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Management Information Base

When SNMP devices send SNMP messages to the management console (the device managing SNMP messages), it stores information in the MIB.

Mbps

Megabits per second.

MD5

MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See “Auto-negotiation” on page 2.

MIB

See “Management Information Base” on page 10.

Multicasting

To transmit a message to specific recipients across a network. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks. Standards are being developed to support multicasting over a TCP/IP network such as the Internet. These standards, IP Multicast and Mbone, will allow users to easily join multicast groups. Note that multicasting refers to sending a message to a select group whereas broadcasting refers to sending a message to everyone connected to a network. The terms multicast and narrowcast are often used interchangeably, although narrowcast usually refers to the business model whereas multicast refers to the actual technology used to transmit the data.

Multiplexing

A function within a layer that interleaves the information from multiple connections into one connection.

MUX

See “Multiplexing” on page 11.

N

netmask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

nm

Nanometer (1 x 10e⁹) meters.

non-stub area

Resource-intensive OSPF area that carries a default route, static routes, intra-area routes, interarea routes, and external routes. Non-stub areas are the only OSPF areas that can have virtual links configured across

them, and are the only areas that can contain an ASBR. Compare with stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

O

Open Systems Interconnection

OSI is a seven (7) layer architecture model for communications systems developed by the ISO for the interconnection of data communications systems. Each layer uses and builds on the services provided by those below it.

OSI

See “Open Systems Interconnection” on page 12.

P

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

PDU

See “Protocol Data Unit” on page 13.

PHY

The OSI Physical Layer: The physical layer provides for transmission of cells over a physical medium connecting two ATM devices. This physical layer is comprised of two sublayers: the Physical Medium Dependent (PMD) sublayer, and the Transmission Convergence (TC) sublayer.

PMC

Packet Mode Channel.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

Port Mirroring

Also known as a roving analysis port. This is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely. An administrator configures port mirroring by assigning a port from which to copy all packets and another port where those packets will be sent. A

packet bound for or heading away from the first port will be forwarded onto the second port as well. The administrator places a protocol analyzer on the port receiving the mirrored data to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port. The monitor port may be a port on the same SwitchModule with an attached RMON probe, a port on a different SwitchModule in the same hub, or the SwitchModule processor. Port mirroring can consume significant CPU resources while active. Better choices for long-term monitoring may include a passive tap like an optical probe or an Ethernet repeater.

Port monitoring

The ability to monitor the traffic passing through a port on a device to analyze network characteristics and perform troubleshooting.

Port speed

The speed that a port on a device uses to communicate with another device or the network.

Port trunking

The ability to combine multiple ports on a device to create a single, high-bandwidth connection.

Protocol

A set of rules for communication between devices on a network.

Protocol Data Unit

PDU is a packet of data passed across a network. The term implies a specific layer of the OSI model and a specific protocol.

Q

QoS

See “Quality of Service” on page 13.

Quality of Service

QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RADIUS

Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.

Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Resource Reservation Setup Protocol

RSVP is a new Internet protocol being developed to enable the Internet to support specified Qualities-of-Service (QoS). Using RSVP, an application will be able to reserve resources along a route from source to destination. RSVP-enabled routers will then schedule and prioritize packets to meet the prioritization assigned by QoS. RSVP is a chief component of a new type of Internet being developed, known broadly as an integrated services Internet. The general idea is to enhance the Internet to support transmission of real-time data.

RFC

The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet. The official specification documents of the Internet Protocol suite that are defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG) are recorded and published as *standards track* RFCs.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

RMON

Short for remote monitoring, a network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it. The newest version of RMON, RMON 2, provides data about traffic at the network layer in addition to the physical layer. This allows administrators to analyze traffic by protocol.

RSVP

See “Resource Reservation Setup Protocol” on page 14.

S

Simple Network Management Protocol

SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. The versions have the following differences:

SNMPv1 (full): Security is based on community strings.

SNMPsec (historic): Security is based on parties. Few, if any, vendors implemented this version of the protocol, which is now largely forgotten.

SNMPv2p (historic): For this version, much work was done to update the SNMPv1 protocol and the SMIV1, and not just security. The result was updated protocol operations, new protocol operations and data types, and party-based security from SNMPsec.

SNMPv2c (experimental): This version of the protocol is called community string-based SNMPv2. It is an update of the protocol operations and data types of SNMPv2p, and uses community-based security from SNMPv1.

SNMPv2u (experimental): This version of the protocol uses the protocol operations and data types of SNMPv2c and security based on users.

SNMPv2* (experimental): This version combined the best features of SNMPv2p and SNMPv2u. (It is also called SNMPv2star.) The documents defining this version were never published as RFCs.

SNMPv3 (proposed): This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*, and updated after much review. The documents defining this protocol will soon be published as RFCs.

SimpleX signaling

SX is one of IEEE 802.3's designations for media. For example, 1000SX indicates 1000 gigabit Ethernet over "short haul" or "short wavelength" optical fiber.

SMII

Serial Media Independent Interface.

SNMP

See "Simple Network Management Protocol" on page 14.

Spanning Tree

A technique that detects loops in a network and logically blocks the redundant paths, ensuring that only one route exists between any two LANs.

Spanning Tree Protocol (STP)

A protocol that finds the most efficient path between segments of a multi-looped, bridged network. STP allows redundant switches and bridges to be used for network resilience, without the broadcast storms associated with looping. If a switch or bridge falls, a new path to a redundant switch or bridge is opened.

SRAM

Static Random Access Memory.

STP

Spanning Tree Protocol. See “802.1D” on page 1 for more information.

stub area

OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry external routes. Virtual links cannot be configured across a stub area, and they cannot contain an ASBR. Compare with non-stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

Subnet Mask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

SX

See “SimpleX signaling” on page 15.

T

Telnet

A character-based UNIX application that enables users with a Telnet server account to log on to a UNIX computer and utilize its resources.

TFTP

See “Trivial File Transfer Protocol” on page 16.

Telnet

A TCP/IP application protocol that provides a virtual terminal service, allowing a user to log into another computer system and access a device as if the user were connected directly to the device.

Traffic prioritization

Giving time-critical data traffic a higher quality of service over other, non-critical data traffic.

Trivial File Transfer Protocol

TFTP is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP, a direct protocol used to communicate datagrams over a network with little error recovery) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trunking

The process of combining a set of trunks that are traffic-engineered as a unit for the establishment of connections between switching systems in which all of the communications paths are interchangeable.

U

USP

An abbreviation that represents Unit, Slot, Port.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

V

Virtual Local Area Network

Operating at the Data Link Layer (Layer 2 of the OSI model), the VLAN is a means of parsing a single network into logical user groups or organizations, as if they physically resided on a dedicated LAN segment of their own. In reality, this virtually defined community may have individual members peppered across a large, extended LAN. The VLAN identifier is part of the 802.1Q tag, which is added to an Ethernet frame by an 802.1Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first three bits of the 802.1Q tag are used by 802.1P to establish priority for the packet.

VLAN

See “Virtual Local Area Network” on page 17.

W

WAN

See “Wide Area Network” on page 18.

Web

Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

X

XModem

One of the most popular file transfer protocols (FTPs). Xmodem is fairly effective at detecting errors. It sends blocks of data together with a checksum and then waits for acknowledgment of the block's receipt. The waiting slows down the rate of data transmission considerably, but it ensures accurate transmission. Xmodem can be implemented either in software or in hardware. Many modems, and almost all communications software packages, support Xmodem. However, it is useful only at relatively slow data transmission speeds (less than 4,800 bps). Enhanced versions of Xmodem that work at higher transmission speeds are known as Ymodem and Zmodem.

A

Address Resolution Protocol. See ARP

ARP

- cache, displaying 7-3

authentication

- login create 7-70
- login delete 7-71
- login set 7-71
- show login info 7-73
- show login users 7-73

Authentication Flag 7-21

Auto MDI/MDI-X 10-2

Auto Uplink 10-2

B

baud rate 7-16

boot code 7-79

Bootstrap Protocol (BOOTP) 7-14

broadcasts

- broadcast storm recovery mode 7-24
- broadcast storm trap 7-21

C

Cat5 cable 10-3

clear commands

- clear config 7-78
- clear pass 7-78
- clear radius stats 7-65
- clear traplog 7-78
- clear vlan 7-78

COM Port Selection 4-2

config commands

- config dot1x adminmode 7-65
- config dot1x defaultlogin 7-72
- config dot1x login 7-72
- config dot1x port controlldir 7-66
- config dot1x port controlmode 7-66
- config dot1x port detailed 7-68
- config dot1x port initialize 7-65
- config dot1x port maxrequests 7-67
- config dot1x port quietperiod 7-66
- config dot1x port reauthenable 7-68

- config dot1x port reauthenticate 7-65
- config dot1x port reauthperiod 7-67
- config dot1x port servertimeout 7-67
- config dot1x port stats 7-69, 7-70
- config dot1x port summary 7-68
- config dot1x port supptimeout 7-67
- config dot1x port transmitperiod 7-67
- config dot1x port users add 7-72
- config dot1x port users remove 7-72
- config dot1x summary 7-68
- config forwardingdb agetime 7-23
- config garp gmrp adminmode 7-36
- config lags addport 7-27
- config lags adminmode 7-28
- config lags create 7-27
- config lags deleteport 7-27
- config lags linktrap 7-28
- config lags name 7-28
- config lags remove 7-28
- config lags stpmode 7-28
- config login session 7-58
- config macfilter 7-43
- config macfilter adddest 7-45
- config macfilter addsrc 7-44
- config macfilter deldest 7-45
- config macfilter delsrc 7-44
- config macfilter remove 7-44
- config mirroring create 7-42
- config mirroring delete 7-43
- config mirroring mode 7-43
- config network ip 7-14
- config network macaddr 7-13
- config network mactype 7-14
- config network netmask 7-14
- config network webmode 7-14, 7-15
- config port admin-mode 7-25
- config port autoneg 7-26
- config port lacp mode 7-26
- config port linktrap 7-25, 7-26
- config port physical-mode 7-26
- config prompt 7-15
- config protocol create 7-33
- config protocol delete 7-33
- config protocol interface add 7-35
- config protocol interface remove 7-35
- config protocol protocol add 7-34
- config protocol protocol remove 7-34
- config protocol vlan add 7-34

- config protocol vlan remove 7-34
- config radius accounting mode 7-59
- config radius accounting server add 7-60
- config radius accounting server port 7-60
- config radius accounting server remove 7-60
- config radius accounting server secret 7-60
- config radius maxretransmit 7-59
- config radius server add 7-61
- config radius server msgauth 7-62
- config radius server port 7-61
- config radius server primary 7-62
- config radius server remove 7-61
- config radius server secret 7-61
- config radius timeout 7-59
- config serial baudrate 7-16
- config serial timeout 7-16
- config servicePort gateway 7-16
- config servicePort ip 7-16
- config snmpcommunity add 7-18
- config snmpcommunity delete 7-18
- config snmpcommunity ip 7-18
- config snmpcommunity ipmask 7-18
- config snmpcommunity mode 7-17
- config snmpcommunity status 7-19
- config snmptrap add 7-19
- config snmptrap delete 7-19
- config snmptrap ip 7-20
- config snmptrap status 7-20
- config switchconfig broadcast 7-24
- config switchconfig flowcontrol 7-24
- config syscontact 7-3
- config syslocation 7-3
- config sysname 7-2
- config telnet maxsessions 7-22
- config telnet status 7-22
- config telnet timeout 7-22
- config trapflags authentication 7-21
- config trapflags bcaststorm 7-21
- config trapflags linkstatus 7-21
- config trapflags multiuser 7-21
- config trapflags stp 7-21
- config users add 7-56
- config users defaultlogin 7-72
- config users delete 7-57
- config users login 7-73
- config users passwd 7-57
- config users snmpv3 accessmode 7-58
- config users snmpv3 authentication 7-57

- config users snmpv3 encryption 7-57
- config vlan add 7-30
- config vlan delete 7-30
- config vlan garp gvarp 7-37
- config vlan garp jointime 7-37
- config vlan garp leavealltime 7-38
- config vlan garp leavetime 7-37
- config vlan interface acceptframe 7-32
- config vlan makestatic 7-31
- config vlan name 7-30
- config vlan participation 7-31
- config vlan ports gvrp 7-37
- config vlan ports ingressfilter 7-33
- config vlan ports pvid 7-32
- config vlan ports tagging 7-31
- igmpsnooping adminmode 7-39
- igmpsnooping groupmembershipinterval 7-39
- igmpsnooping interface mode 7-40
- igmpsnooping maxresponse 7-39
- igmpsnooping mcrtr_expiretime 7-39

- config sysname 7-2

- configuration changes, saving 7-58, 7-74

- configuration reset 7-78

- console port 4-1

- conventions

- typography 1-2

- crossover cable 10-2

D

- Device Configuration Commands 7-23

- device configuration commands

- 201 commands 7-23 to 7-38, ?? to 7-38

- DHCP 7-14

- Direct Console Access 4-1

- Documentation updates 1-2

- dot1x

- adminmode 7-65

- aport initialize 7-65

- config defaultlogin 7-72

- config login 7-72

- config port users add 7-72

- config port users remove 7-72

- port controldir 7-66

- port controlmode 7-66

- port detailed 7-68
- port maxrequests 7-67
- port quietperiod 7-66
- port reauthenable 7-68
- port reauthenticate 7-65
- port reauthperiod 7-67
- port servertimeout 7-67
- port stats 7-69, 7-70
- port summary 7-68
- port transmitperiod 7-67
- show port users 7-73
- summary 7-68
- supptimeout 7-67
- downloading
 - data types, setting 7-77
 - file names, setting 7-77
 - file paths, setting 7-77
 - IP addresses, setting 7-77
 - mode, setting 7-76
 - starting a transfer 7-78
- duplex settings 7-26
- Dynamic Host Configuration Protocol. See DHCP

F

- flow control 7-24
- forwarding database
 - show forwardingDB command 7-3, 7-4
- frame acceptance mode 7-32

G

- garp
 - gmrp adminmode 7-36
 - gmrp interface 7-36
 - interface 7-35
 - show info 7-35
- GVRP
 - enabling or disabling 7-37
 - join time 7-37
 - leave time 7-37

H

- How to Use This Document 1-1
- http

Index

- [//www.netgear.com/](http://www.netgear.com/) 1-ii
- Hyper Terminal 4-2

I

- IEEE 802.1Q 7-32
- igmpsnooping
 - adminmode 7-39
 - groupmembershipinterval 7-39
 - interface mode 7-40
 - maxresponse 7-39
 - mcrptreptime 7-39
 - show 7-38
- ingress filtering 7-33
- inventory 7-1

J

- join time 7-37

L

- LAGs
 - adding ports to 7-27
 - configuring 7-27
 - deleting ports from 7-27
 - enabling or disabling 7-28
 - link traps 7-28
 - name 7-28
 - removing 7-28
 - STP mode 7-28
 - summary information 7-26
- leave time 7-37, 7-38
- link aggregations. See LAGs
- link traps
 - interface 7-25, 7-26
 - LAG 7-28
 - switch 7-21
- Log in 5-2
- logout command 7-74

M

- MAC addresses 7-13, 7-14
- macfilter

- adddest 7-45
- addsrc 7-44
- create 7-43
- deldest 7-45
- delsrc 7-44
- remove 7-44
- show 7-43
- Management Access 2-1
- management commands
 - 201 commands 7-13 to 7-22
- MDI/MDI-X 10-2
- MDI/MDI-X wiring 10-11
- mfdb
 - gmrp 7-40
 - igmpsnooping 7-41
 - staticfiltering 7-41
 - stats 7-42
 - table 7-40
- mirroring
 - create 7-42
 - delete 7-43
 - mode 7-43
 - show 7-42
- msg log
 - displaying 7-12
- Multiple User traps 7-21

N

- network configuration commands
 - 201 commands 7-13 to 7-22
- network configuration protocols 7-14
- network contact 7-3
- Non-Volatile Random Access Memory (NVRAM)
 - 7-58, 7-74

P

- passwords
 - changing user 7-57
 - resetting all 7-78
- PDU 7-37, 7-38
- ping command 7-80
- ports

- adding to LAGs 7-27
- administrative mode 7-25
- autoneg 7-26
- deleting from LAGs 7-27
- frame acceptance mode 7-32
- GVRP 7-37
- information 7-24
- ingress filtering 7-33
- lacp mode 7-26
- link traps 7-25, 7-26
- physical mode 7-26
- statistics, related 201 commands 7-4, 7-9
- tagging 7-31
- VLAN IDs 7-32
- VLAN information 7-32

Product updates 1-2

prompt, changing 7-15

protocol

- create 7-33
- delete 7-33
- interface add 7-35
- interface remove 7-35
- protocol add 7-34
- protocol remove 7-34
- show 7-33
- vlan ad 7-34
- vlan remove 7-34

Protocol Data Units. See PDUs

R

radius

- accounting mode 7-59
- accounting server add 7-60
- accounting server port 7-60
- accounting server remove 7-60
- accounting server secret 7-60
- accounting stats 7-64
- accounting summary 7-64
- clear stats 7-65
- maxretransmit 7-59
- server add 7-61
- server msgauth 7-62
- server port 7-61
- server primary 7-62
- server remove 7-61
- server secret 7-61

- server stats 7-63
- server summary 7-62
- stats 7-65
- summary 7-62
- timeout 7-59
- reset system command 7-79
- root traps 7-21
- routing
 - default router IP address, setting 7-16

S

- save config command 7-58, 7-74
- Security Commands 7-58
- security commands 7-58 to 7-74
- serial communication settings 7-15, 7-16
- service port configuration
 - 201 commands 7-16
- sessions
 - closing 7-58, 7-74
 - displaying 7-58
- show commands
 - show arp switch 7-3
 - show authentication login create 7-70
 - show authentication login delete 7-71
 - show authentication login info 7-73
 - show authentication login set 7-71
 - show authentication login users 7-73
 - show dot1x port users 7-73
 - show forwardingDB 7-3, 7-4
 - show forwardingdb agetime 7-23
 - show garp gmrp interface 7-36
 - show garp info 7-35
 - show garp interface 7-35
 - show igmpsnooping 7-38
 - show inventory 7-1
 - show lags summary 7-26
 - show login session 7-58
 - show macfilter 7-43
 - show mfdb gmrp 7-40
 - show mfdb igmpsnooping 7-41
 - show mfdb staticfiltering 7-41
 - show mfdb stats 7-42
 - show mfdb table 7-40
 - show mirroring 7-42

- show msglog 7-12
- show network 7-13
- show port 7-24
- show protocol 7-33
- show radius accounting stats 7-64
- show radius accounting summary 7-64
- show radius server stats 7-63
- show radius server summary 7-62
- show radius stats 7-65
- show radius summary 7-62
- show serial 7-15
- show servicePort 7-16
- show snmpcommunity 7-17
- show snmptrap 7-19
- show spanningtree adminmode 7-46
- show spanningtree bridge 7-48
- show spanningtree bridge forwarddelay 7-49
- show spanningtree bridge hellotime 7-49
- show spanningtree bridge maxage 7-49
- show spanningtree bridge priority 7-49
- show spanningtree configuration name 7-47
- show spanningtree configuration revision 7-47
- show spanningtree cst detailed 7-49
- show spanningtree cst port detailed 7-51
- show spanningtree cst port edgeport 7-52
- show spanningtree cst port pathcost 7-51
- show spanningtree cst port priority 7-52
- show spanningtree cst port summary 7-50
- show spanningtree forceversion 7-47
- show spanningtree mst create 7-52
- show spanningtree mst delete 7-52
- show spanningtree mst detailed 7-54
- show spanningtree mst port detailed 7-55
- show spanningtree mst port pathcost 7-53
- show spanningtree mst port priority 7-54
- show spanningtree mst port summary 7-55
- show spanningtree mst priority 7-53
- show spanningtree mst summary 7-54
- show spanningtree mst vlan add 7-53
- show spanningtree mst vlan remove 7-53
- show spanningtree port 7-47, 7-48
- show spanningtree port mode 7-48
- show spanningtree summary 7-46
- show stats port detailed 7-4
- show stats port summary 7-9
- show stats switch detailed 7-10
- show stats switch summary 7-11
- show switchconfig 7-24

- show sysinfo 7-2
- show telnet 7-22
- show trapflags 7-20
- show traplog 7-12
- show users 7-56
- show users authentication 7-74
- show vlan detailed 7-29
- show vlan interface 7-32
- show vlan summary 7-29, 7-55

SNMP 2-2

SNMP communities

- access rights 7-17
- adding 7-18
- client IP masks 7-18
- deleting 7-18
- information 7-17
- IP address 7-18
- status 7-19

SNMP traps

- deleting 7-19
- information 7-19
- IP addresses 7-20
- names 7-19
- status 7-20

spanningtree

- adminmode 7-46
- bridge 7-48
- bridge forwarddelay 7-49
- bridge hellotime 7-49
- bridge maxage 7-49
- bridge priority 7-49
- configuration name 7-47
- configuration revision 7-47
- cst detailed 7-49
- cst port detailed 7-51
- cst port edgeport 7-52
- cst port pathcost 7-51
- cst port priority 7-52
- cst port summary 7-50
- forceversion 7-47
- mst create 7-52
- mst delete 7-52
- mst detailed 7-54
- mst port detailed 7-55
- mst port pathcost 7-53
- mst port priority 7-54
- mst port summary 7-55

- mst priority 7-53
- mst summary 7-54
- mst vlan add 7-53
- mst vlan remove 7-53
- port 7-47
- port migrationcheck 7-48
- port mode 7-48
- summary 7-46
- vlan 7-55

speeds 7-26

statistics

- port, related 201 commands 7-4, 7-9
- switch, related 201 commands 7-10, 7-11

STP

- settings for LAGs 7-28
- traps 7-21

switch

- connectivity 7-3
- information, related 201 commands 7-2, 7-24
- inventory 7-1
- IP address 7-14, 7-16
- location 7-3
- msg log 7-12
- name 7-2
- resetting 7-79
- serial communication settings 7-15
- statistics, related 201 commands 7-10, 7-11
- trap log 7-12

system administrator 7-3

System Information and Statistics Commands 7-1

- system information and statistics commands
- 201 commands 7-1 to 7-12

System Utilities 7-74

- system utilities 7-74 to 7-80

T

tagging 7-31

telnet

- maximum number of sessions 7-22
- sessions, closing 7-58, 7-74
- sessions, displaying 7-58
- sessions, timeouts 7-22
- settings 7-22
- status 7-25

- TFTP
 - setting as download mode 7-76
 - setting as upload mode 7-74
- timeouts
 - forwardingdb 7-23
 - serial 7-16
- TIP 4-2
- topology change notification traps 7-21
- transfer commands
 - transfer download datatype 7-77
 - transfer download filename 7-77
 - transfer download mode 7-76
 - transfer download path 7-77
 - transfer download serverip 7-77
 - transfer download start 7-78
 - transfer upload datatype 7-76
 - transfer upload filename 7-76
 - transfer upload mode 7-74
 - transfer upload path 7-75
 - transfer upload serverip 7-75
 - transfer upload start 7-76
- trap flags
 - Authentication 7-21
 - broadcast storm 7-21
 - information 7-20
 - Link Up/Down 7-21
 - Multiple User 7-21
 - STP 7-21
- trap log
 - clearing 7-78
 - displaying 7-12
- Trivial File Transfer Protocol. See TFTP
- trunks. See LAGs
- typographical conventions 1-2

U

- uploading
 - file names, setting 7-76
 - file paths, setting 7-75
 - file types, setting 7-76
 - IP addresses, setting 7-75
 - mode, setting 7-74
 - starting a transfer 7-76
- User Account Management Commands 7-56

- user account management commands
 - 201 commands 7-56 to 7-58
- users
 - adding 7-56
 - config defaultlogin 7-72
 - config login 7-73
 - deleting 7-57
 - displaying 7-56
 - passwords 7-57, 7-78
 - show authentication 7-74
 - snmpv3 accessmode 7-58
 - snmpv3 authentication 7-57
 - snmpv3 encryption 7-57

V

- VLANs
 - adding 7-30
 - changing the name of 7-30
 - deleting 7-30
 - details 7-29
 - frame acceptance mode 7-32
 - GVRP 7-37
 - IDs 7-32
 - ingress filtering 7-33
 - jointime 7-37
 - leave all time 7-38
 - leave time 7-37
 - making static 7-31
 - participation in 7-31
 - port information 7-32
 - resetting parameters 7-78
 - summary information 7-29, 7-55
 - tagging 7-31
- VT100 interface 2-1

W

- Web access 7-14, 7-15
- Web Based Management 5-1
- Web connections, displaying 7-58
- Web site 1-2
- Why the Document was Created 1-1

X

XMODEM

setting as download mode 7-76

setting as upload mode 7-74

Z

ZTerm 4-2