

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



NETGEAR

NETGEAR, Inc.

4500 Great America
Parkway

Santa Clara, CA

202-10010-02
December 2004

December 2004, 202-10010-02

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 (NETGEAR 7200 Series 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 NETGEAR 7200 Series 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

Audience	1-1
Why the Document was Created	1-1
How to Use This Document	1-1
Typographical Conventions	1-2
Special Message Formats	1-2
Features of the HTML Version of this Manual	1-3
How to Print this Manual	1-4

Chapter 2

Switch Management Overview

Scope	2-1
Switch Management Overview	2-1

Chapter 3

Administration Console Telnet Interface

Set Up Your Switch Using Direct Console Access	3-1
--	-----

Chapter 4

Web-Based Management Interface

Web Based Management Overview	4-1
How to Log In to the Managed Switch	4-2
Web-Based Management Utility Features	4-3
Interactive Switch Image	4-4
Menus	4-4
System-Wide Popup Menus	4-4
Port-Specific Popup Menus	4-4

Chapter 5

Command Line Interface Structure

CLI Command Format	5-1
Command	5-1
Parameters	5-2
Values	5-2

Conventions	5-3
Annotations	5-4
Chapter 6	
Quick Start up	
Quick Starting the Switch	6-1
System Info and System Setup	6-2
Quick Start up Software Version Information	6-2
Quick Start up Physical Port Data	6-2
Quick Start up User Account Management	6-3
Quick Start up IP Address	6-3
Quick Start up Uploading from Switch to Out-of-Band PC (Only XMODEM)	6-5
Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)	6-6
Quick Start up Downloading from TFTP Server	6-6
Quick Start up Factory Defaults	6-7
Chapter 7	
Mode-based CLI	
Mode-based Topology	7-2
Mode-based Command Hierarchy	7-4
Flow of Operation	7-5
“No” Form of a Command	7-6
Support for “No” Form	7-6
Behavior of Command Help (“?”)	7-6
Chapter 8	
Switching Commands	
System Information and Statistics Commands	8-1
show arp switch	8-1
show eventlog	8-2
show hardware	8-2
show interface	8-2
show interface ethernet	8-4
show logging	8-12
show mac-addr-table	8-12
show msglog	8-13
show running-config	8-14
show sysinfo	8-14

snmp-server	8-14
Management VLAN Commands	8-15
network mgmt_vlan	8-15
Dot1P Commands	8-15
classofservice dot1pmapping	8-15
show classofservice dot1pmapping	8-15
vlan port priority all	8-16
vlan priority	8-16
LAG/Port-Channel (802.3ad) Commands	8-16
port-channel staticcapability	8-16
no port-channel staticcapability	8-16
show port-channel brief	8-17
Management Commands	8-17
bridge aging-time	8-17
no bridge aging-time	8-18
mtu	8-18
no mtu	8-18
network javamode	8-19
no network javamode	8-19
network mac-address	8-19
network mac-type	8-19
no network mac-type	8-20
network parms	8-20
network protocol	8-20
remotecon maxsessions	8-20
no remotecon maxsessions	8-21
remotecon timeout	8-21
no remotecon timeout	8-21
serial baudrate	8-21
no serial baudrate	8-22
serial timeout	8-22
no serial timeout	8-22
set prompt	8-22
show forwardingdb agetime	8-22
show network	8-23

show remotecon	8-24
show serial	8-24
show snmpcommunity	8-25
show snmptrap	8-26
show trapflags	8-27
snmp-server community	8-27
no snmp-server community	8-28
snmp-server community ipaddr	8-28
no snmp-server community ipaddr	8-28
snmp-server community ipmask	8-29
no snmp-server community ipmask	8-29
snmp-server community mode	8-29
no snmp-server community mode	8-29
snmp-server community ro	8-30
snmp-server community rw	8-30
snmp-server enable traps	8-30
no snmp-server enable traps	8-30
snmp-server enable traps bcaststorm	8-30
no snmp-server enable traps bcaststorm	8-31
snmp-server enable traps linkmode	8-31
no snmp-server enable traps linkmode	8-31
snmp-server enable traps multiusers	8-31
no snmp-server enable traps multiusers	8-32
snmp-server enable traps stpmode	8-32
no snmp-server enable traps stpmode	8-32
snmptrap	8-32
no snmptrap	8-32
snmptrap ipaddr	8-33
snmptrap mode	8-33
no snmptrap mode	8-33
telnet	8-33
no telnet	8-34
HTTP Commands	8-34
ip http secure-port	8-34
no ip http secure-port	8-34

ip http secure-protocol	8-34
no ip http secure-protocol	8-34
ip http secure-server	8-35
no ip http secure-server	8-35
ip http server	8-35
no ip http server	8-35
show ip http	8-36
Secure Shell (SSH) Commands	8-36
ip ssh	8-36
no ip ssh	8-36
ip ssh protocol	8-36
show ip ssh	8-37
Device Configuration Commands	8-37
addport	8-37
auto-negotiate	8-37
no auto-negotiate	8-38
auto-negotiate all	8-38
no auto-negotiate all	8-38
delete interface	8-38
deleteport	8-38
deleteport	8-39
monitor session	8-39
no monitor session	8-39
monitor session mode	8-39
no monitor session mode	8-40
port lacpmode	8-40
no port lacpmode	8-40
port lacpmode all	8-40
no port lacpmode all	8-40
port-channel	8-40
port-channel adminmode	8-41
no port-channel adminmode	8-41
port-channel linktrap	8-41
no port-channel linktrap	8-41
port-channel name	8-42

protocol group	8-42
no protocol group	8-42
protocol vlan group	8-42
no protocol vlan group	8-43
protocol vlan group all	8-43
no protocol vlan group all	8-43
set garp timer join	8-43
no set garp timer join	8-44
set garp timer join all	8-44
no set garp timer join all	8-44
set garp timer leave	8-44
no set garp timer leave	8-45
set garp timer leave all	8-45
no set garp timer leave all	8-45
set garp timer leaveall	8-46
no set garp timer leaveall	8-46
set garp timer leaveall all	8-46
no set garp timer leaveall all	8-46
set gmrp adminmode	8-47
no set gmrp adminmode	8-47
set gmrp interfacemode	8-47
no set gmrp interfacemode	8-47
set gmrp interfacemode all	8-48
no set gmrp interfacemode all	8-48
set gvrp adminmode	8-48
no set gvrp adminmode	8-48
set gvrp interfacemode	8-48
no set gvrp interfacemode	8-49
set gvrp interfacemode all	8-49
no set gvrp interfacemode all	8-49
set igmp	8-49
no set igmp	8-50
set igmp	8-50
no set igmp	8-50
set igmp groupmembershipinterval	8-50

no set igmp groupmembershipinterval	8-50
set igmp interfacemode all	8-51
no set igmp interfacemode all	8-51
set igmp maxresponse	8-51
no set igmp maxresponse	8-51
set igmp mcrtrexpiretime	8-52
no set igmp mcrtrexpiretime	8-52
show garp	8-52
show gmrp configuration	8-52
show gvrp configuration	8-54
show igmpsnooping	8-55
show mac-address-table gmrp	8-56
show mac-address-table igmpsnooping	8-56
show mac-address-table multicast	8-57
show mac-address-table static	8-57
show mac-address-table staticfiltering	8-58
show mac-address-table stats	8-58
show monitor	8-59
show port	8-59
show port protocol	8-60
show port-channel	8-60
show storm-control	8-61
show vlan	8-61
show vlan brief	8-63
show vlan port	8-63
shutdown	8-64
no shutdown	8-64
shutdown all	8-64
no shutdown all	8-65
snmp trap link-status	8-65
no snmp trap link-status	8-65
snmp trap link-status all	8-65
no snmp trap link-status all	8-65
spanning-tree	8-66
spanning-tree bpdumigrationcheck	8-66

no spanning-tree bpdumigrationcheck	8-66
speed	8-67
speed all	8-67
storm-control broadcast	8-67
no storm-control broadcast	8-68
storm-control flowcontrol	8-69
no storm-control flowcontrol	8-69
vlan	8-69
no vlan	8-69
vlan acceptframe	8-70
no vlan acceptframe	8-70
vlan ingressfilter	8-70
no vlan ingressfilter	8-70
vlan makestatic	8-71
vlan name	8-71
no vlan name	8-71
vlan participation	8-71
vlan participation all	8-72
vlan port acceptframe all	8-72
no vlan port acceptframe all	8-73
vlan port ingressfilter all	8-73
no vlan port ingressfilter all	8-73
vlan port pvid all	8-73
no vlan port pvid all	8-73
vlan port tagging all	8-74
no vlan port tagging all	8-74
vlan protocol group	8-74
vlan protocol group add protocol	8-74
no vlan protocol group add protocol	8-75
vlan protocol group remove	8-75
vlan pvid	8-75
no vlan pvid	8-75
vlan tagging	8-75
no vlan tagging	8-76
Spanning Tree Commands	8-76

show spanning-tree	8-76
show spanning-tree interface	8-77
show spanning-tree mst detailed	8-78
show spanning-tree mst port detailed	8-79
LAN	8-79
show spanning-tree mst port summary	8-80
show spanning-tree mst summary	8-81
show spanning-tree summary	8-81
show spanning-tree vlan	8-81
spanning-tree	8-82
no spanning-tree	8-82
spanning-tree configuration name	8-82
no spanning-tree configuration name	8-82
spanning-tree configuration revision	8-83
no spanning-tree configuration revision	8-83
spanning-tree edgeport	8-83
no spanning-tree edgeport	8-83
spanning-tree forceversion	8-83
no spanning-tree forceversion	8-84
spanning-tree forward-time	8-84
no spanning-tree forward-time	8-84
spanning-tree hello-time	8-85
no spanning-tree hello-time	8-85
spanning-tree max-age	8-85
no spanning-tree max-age	8-85
spanning-tree mst	8-86
no spanning-tree mst	8-86
spanning-tree mst instance	8-87
no spanning-tree mst instance	8-87
spanning-tree mst priority	8-87
no spanning-tree mst priority	8-88
spanning-tree mst vlan	8-88
no spanning-tree mst vlan	8-88
spanning-tree port mode	8-88
no spanning-tree port mode	8-89

spanning-tree port mode all	8-89
no spanning-tree port mode all	8-89
User Account Management Commands	8-89
disconnect	8-89
show login session	8-89
show users	8-90
users name	8-91
no users name	8-91
users passwd	8-91
no users passwd	8-92
users snmpv3 accessmode	8-92
no users snmpv3 accessmode	8-92
users snmpv3 authentication	8-92
no users snmpv3 authentication	8-93
users snmpv3 encryption	8-93
no users snmpv3 encryption	8-93
Security Commands	8-93
authentication login	8-94
no authentication login	8-94
clear dot1x statistics	8-95
clear radius statistics	8-95
dot1x defaultlogin	8-95
dot1x initialize	8-95
dot1x login	8-95
dot1x max-req	8-96
no dot1x max-req	8-96
dot1x port-control	8-96
no dot1x port-control	8-97
dot1x port-control All	8-97
no dot1x port-control All	8-97
dot1x re-authenticate	8-97
dot1x re-authentication	8-98
no dot1x re-authentication	8-98
dot1x system-auth-control	8-98
no dot1x system-auth-control	8-98

dot1x timeout	8-98
no dot1x timeout	8-99
dot1x user	8-100
no dot1x user	8-100
radius accounting mode	8-100
no radius accounting mode	8-100
radius server host	8-100
no radius server host	8-101
radius server key	8-102
radius server msgauth	8-102
radius server primary	8-102
radius server retransmit	8-102
no radius server retransmit	8-103
radius server timeout	8-103
no radius server timeout	8-103
show accounting	8-103
show authentication	8-105
show authentication users	8-105
show dot1x	8-105
show dot1x users	8-108
show radius	8-108
show radius statistics	8-109
show users authentication	8-110
users defaultlogin	8-111
users login	8-111
System Utilities	8-111
clear config	8-111
clear counters	8-112
clear igmpsnooping	8-112
clear pass	8-112
clear port-channel	8-112
clear traplog	8-112
clear vlan	8-113
copy	8-113
logout	8-114

ping	8-114
reload	8-114

Chapter 9

DHCP Server Commands

DHCP Server Configuration Commands	9-1
client-identifier	9-1
no client-identifier	9-1
client-name	9-1
no client-name	9-1
default-router	9-2
no default-router	9-2
dns-server	9-2
no dns-server	9-2
hardware-address	9-3
no hardware-address	9-3
host	9-3
no host	9-3
ip dhcp excluded-address	9-4
no ip dhcp excluded-address	9-4
ip dhcp ping packets	9-4
no ip dhcp ping packets	9-4
ip dhcp pool	9-5
no ip dhcp pool	9-5
lease	9-5
no lease	9-5
network	9-6
no network	9-6
service dhcp	9-6
no service dhcp	9-6
DHCP Server Show Commands	9-6
show ip dhcp binding	9-7
show ip dhcp global configuration	9-7
show ip dhcp pool configuration	9-7
show ip dhcp server statistics	9-8
DHCP Server Clear Commands	9-9

clear ip dhcp binding	9-9
clear ip dhcp server statistics	9-9

Appendix A
IS CLI Mapping

Appendix B
Cabling Guidelines

Fast Ethernet Cable Guidelines	11-1
Category 5 Cable	11-2
Category 5 Cable Specifications	11-2
Twisted Pair Cables	11-3
Patch Panels and Cables	11-4
Using 1000BASE-T Gigabit Ethernet over Category 5 Cable	11-5
Cabling	11-5
Near End Cross Talk (NEXT)	11-6
Patch Cables	11-6
RJ-45 Plug and RJ-45 Connectors	11-6
Conclusion	11-8

Appendix C
Glossary

Numeric	12-1
A	12-2
B	12-3
C	12-4
D	12-4
E	12-6
F	12-6
G	12-7
H	12-8
I	12-8
L	12-10
M	12-11
N	12-12
O	12-13
P	12-13
Q	12-14

R	12-15
S	12-16
T	12-17
U	12-18
V	12-18
W	12-19
X	12-19

Chapter 1

About This Guide

Thank you for purchasing the NETGEAR™ 7200 Series 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 7200 Series L2 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 7200 Series L2 Switch software. It is intended to provide an understanding of the configuration options of 7200 Series 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 7000 Series L3 Managed Switch software. The commands can be accessed from the CLI, telnet, and Web interfaces.

- [Chapter 6, “Quick Start up”](#) details the procedure to quickly become acquainted with the 7000 Series L3 Managed Switch Software.
- [Chapter 8, “Switching Commands”](#) describes the Switching commands.

Note: Refer to the release notes for the 7000 Series L3 Managed Switch Software application level code. The release notes detail the platform specific functionality of the Switching, Routing, SNMP, Config, Management, and Bandwidth Provisioning 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 7200 Series L2 Switch according to these specifications:

Table 1-1. Manual Specifications

Product Version	NETGEAR 7200 Series Layer 2 Managed Switch
Manual Publication Date	December 2004

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

Features of the HTML Version of this Manual

The HTML version of this manual includes these features.

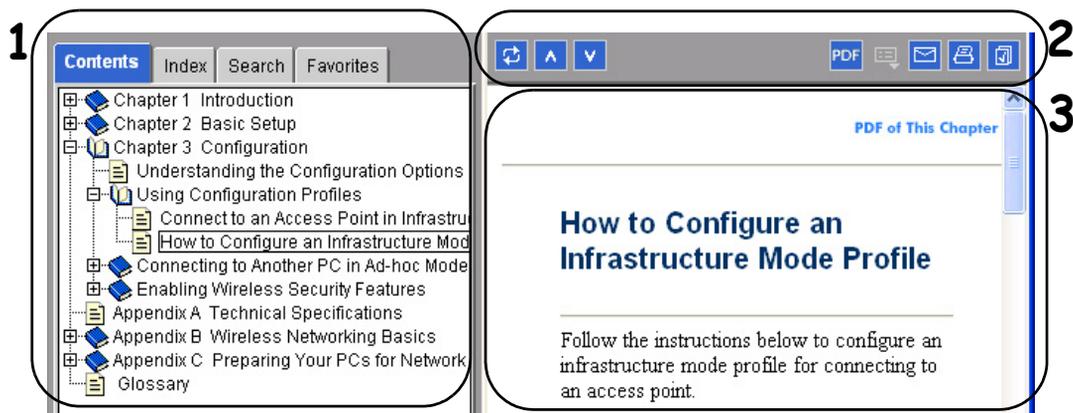


Figure Preface -2: HTML version of this manual

- 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 NETGEAR 7200 Series Layer 2 Managed Switch.

- Management Access Overview
- SNMP Access
- Protocols

Scope

The NETGEAR 7200 Series Layer 2 Managed Switch software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2 or 3 information contained in the frames.
- Provide 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 NETGEAR 7200 Series Layer 2 Managed Switch provides a flexible solution to these ever-increasing needs.

The NETGEAR 7200 Series Layer 2 Managed Switch provides the network administrator with a set of comprehensive management functions for managing both the 7200 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 managed switch 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	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Must be near switch or use dial-up connection • Not convenient for remote users • Not graphical
Web browser or Telnet	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Communicates with switch functions at the Management Information Base (MIB) level • Based on open standards 	<ul style="list-style-type: none"> • 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)

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 a 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 will appear. Enter a name for this connection. In the example below, the name of the connection is GSM7224. Click OK.



Figure 3-2: Connection Description

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



Figure 3-3: COM Port Selection

- When the following screen appears, make sure that the port setting are as follows:

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

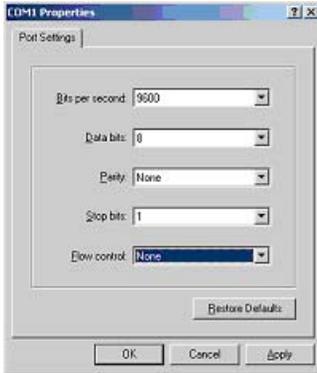


Figure 3-4: Connection Settings

- Click OK.

The HyperTerminal window will open and you should be connected to the switch. If you do not get a welcome screen or a system menu, press 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 4

Web-Based Management Interface

Your NETGEAR 7200 Series 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.

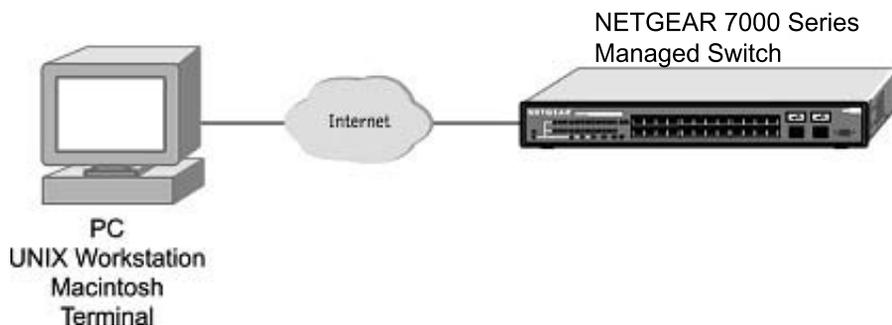


Figure 4-1: Web Management Method

Web Based Management Overview

The menu options available are: System Management, Switch, Routing, Traffic Management, and Smart Wizard. 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 Managed Switch

The NETGEAR 7200 Series 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 managed switch.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Log in to the managed switch using whatever 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 4-2: 7200 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 4-3: 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 7200 Series 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.

- Management
- Switch
- Traffic Management
- Smart Wizard

System-Wide Popup Menus

The 7200 Series 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 7200 Series 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 5

Command Line Interface Structure

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

CLI Command Format

Commands are followed by values, parameters, or both.

Example 1

```
network parms <ipaddr> <netmask> [<gateway>]
```

- **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

```
snmp-server location <loc>
```

- **snmp-server location** is the command name.
- <loc> is the required parameter for the command.

Example 3

```
clear vlan
```

- **clear vlan** is the command name.

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 may be entered in place of the brackets and text inside them.
- *choice1 | choice2*. The | indicates that only one of the parameters should be entered.
- The { } curly braces indicate that a parameter must be chosen from the list of choices.

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 (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 00:06:29:32:81:40.

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 sub-netted 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 number 1. The *<slot/port>* field is composed of a valid slot number and a valid port number separated by a forward slash (/).

logical slot/port

This parameter denotes a logical slot number and logical port number assigned. This is applicable in the case of a port-channel (LAG). The operator can use the logical slot number and the logical port number to configure the port-channel.

Conventions

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

Table 5-1. 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 wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings (“”) are not valid user defined strings.

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 6

Quick Start up

The CLI Quick Start up details procedures to quickly become acquainted with the 7200 Series L2 Switch.

Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the 7200 Series L2 Switch locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. 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, NETGEAR suggests logging into an administrator account.
 - Do not enter a password because there is no password in the default mode.
 - Press the enter key two times.
 - The CLI User EXEC prompt will be displayed.
 - Use “enable” to switch to the Privileged EXEC mode from User EXEC.
 - Use “configure” to switch to the Global Config mode from Privileged EXEC.
 - Use “exit” to return to the previous mode.

System Info and System Setup

Quick Start up Software Version Information

Table 6-1. Quick Start up Software Version Information

Command	Details
<code>show hardware</code> (in Privileged EXEC)	Allows the user to see the software version the device contains
	Software Version - current release software loaded in the switch

Quick Start up Physical Port Data

Table 6-2. Quick Start up Physical Port Data

Command	Details
<code>show port all</code> (in Privileged EXEC)	Displays the Ports
	slot/port
	Type - Indicates if the port is a special type of port
	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 Start up User Account Management

Table 6-3. Quick Start up User Account Management

Command	Details
<code>show users</code> (in Privileged EXEC)	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.
<code>show login session</code> (in User EXEC)	Displays all of the login session information
<code>users passwd <username></code> (in Global Config)	Allows the user to set passwords or change passwords needed to login A prompt will appear after the command is entered 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 will be displayed. User password should not be more than eight characters in length.
<code>copy system:running-config nvram:startup-config</code> (in Privileged EXEC)	This will save passwords and all other changes to the device. If you do not save config, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset
<code>logout</code> (in User EXEC and Privileged EXEC)	Logs the user out of the switch

Quick Start up 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: The user should do a **copy system:running-config nvram:startup-config** after configuring the network parameters so that the configurations are not lost

Table 6-4. Quick Start up IP Address

Command	Details
show network (in User EXEC)	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
	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
	Network Configurations Protocol Current - Indicates which network protocol is being used Default is none
	Management VLAN Id - Specifies VLAN id
	Web Mode - Indicates whether HTTP/Web is enabled.
	Java Mode - Indicates whether java mode is enabled.
network parms (in Privileged EXEC)	network parms <ipaddr> <netmask> [<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

Note: The IP address assigned to **network** in the above table will not be routable. If access to management CPU via the routable interface is desired, use the **ip** command.

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

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

Command	Details
<pre>copy { nvram:startup-config / nvram:errorlog / nvram:msglog / nvram:traplog} <url></pre>	<p>The types are:</p> <ul style="list-style-type: none"> config - configuration file errorlog - error log system trace - system trace traplog - trap log <p>The URL must be specified as:</p> <p>xmodem:filepath/fileName</p>
	<p>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.</p> <p>For example:</p> <p>If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.</p>

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

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

Command	Details
<code>copy <url> {nvram:startup-config system:image}</code>	Sets the download datatype to be an image or config file. The URL must be specified as: xmodem:filepath/fileName
	For example: If the user is using HyperTerminal, the user must specify which file is to be sent to the switch. The Switch will restart automatically once the code has been downloaded.

Quick Start up Downloading from TFTP Server

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

Table 6-7. Quick Start up Downloading from TFTP Server

Command	Details
<code>copy <url> {nvram:startup-config system:image}</code>	Sets the download datatype to be an image or config file. The URL must be specified as: tftp://ipAddr/filepath/fileName. The nvram:startup-config option downloads the config file using tftp and system:image option downloads the code file.

Quick Start up Factory Defaults

Table 6-8. Quick Start up Factory Defaults

Command	Details
clear config	Enter yes when the prompt pops up to clear all the configurations made to the switch.
copy system:running-config nvram:startup-config	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
reload 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.

Chapter 7

Mode-based CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific 7200 Series L2 Switch commands.

- User Exec Mode
- Privileged Exec Mode
- Global Config Mode
- Vlan Mode
- Interface Config Mode
- Line Config Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Table 7-1. Command Mode

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User Exec Mode	This is the first level of access. Perform basic tasks and list system information.	Switch>	Enter Logout command
Privileged Exec Mode	From the User Exec Mode, enter the enable command.	Switch#	To exit this mode, enter exit or press Ctrl-Z.
VLAN Mode	From the Privileged User Exec mode, enter the vlan database command.	Switch (Vlan) #	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.

Table 7-1. Command Mode (continued)

Command Mode	Access Method	Prompt	Exit or Access Next Mode
Global Config Mode	From the Privileged Exec mode, enter the configure command.	Switch (Config)#	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
Interface Config Mode	From the Global Configuration mode, enter the interface config <slot/port> command.	Switch (Interface-"if number")#	To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.
Line Config Mode	From the Global Configuration mode, enter the lineconfig command.	Switch (line) #	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.

Mode-based Topology

The CLI tree is built on a mode concept where the commands are available according to the interface. Some of the modes are depicted in the mode-based CLI Figure 1.

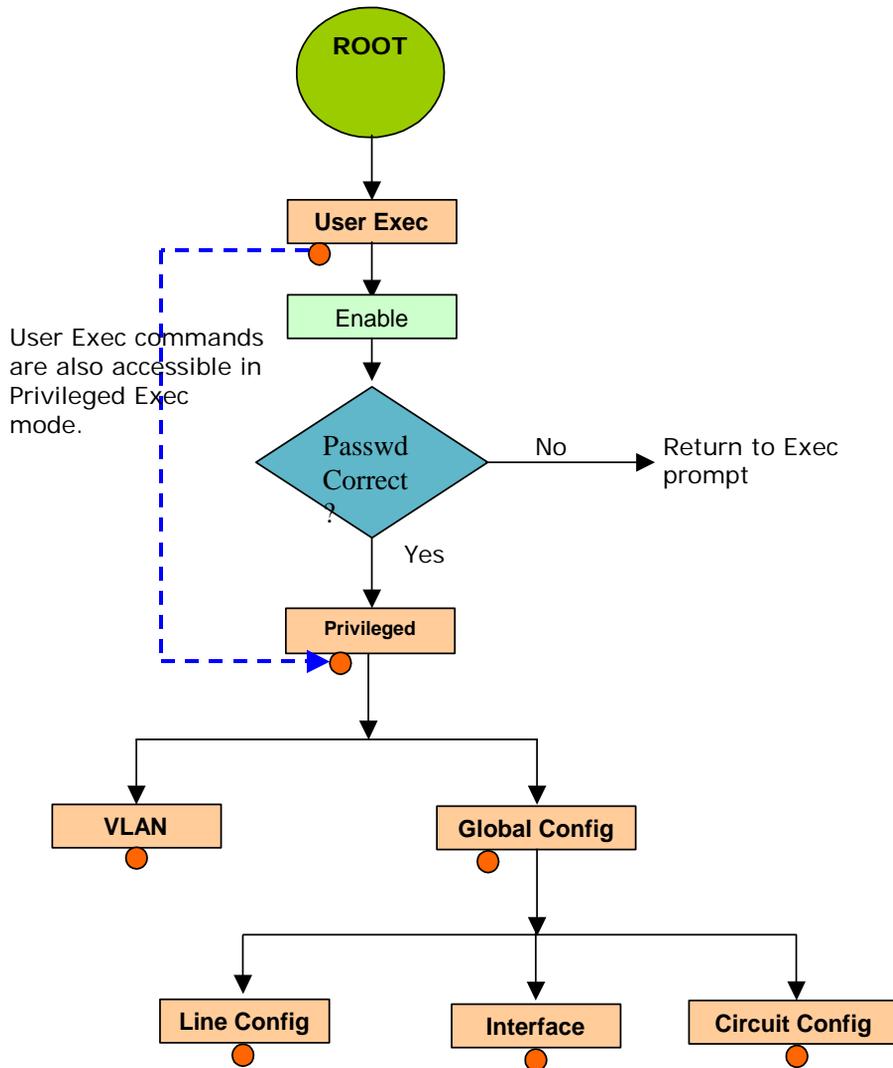


FIGURE 1. Mode-based CLI

Access to all commands in the Privileged Exec mode and below are restricted through a password.

Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode.

The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

- | | |
|-----------------------------|--|
| User Exec Mode | When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is:
Command Prompt: \$(Exec)> |
| Privileged Exec Mode | To have access to the full suite of commands, the operator must enter the Privileged Exec mode. The Privileged Exec mode requires password authentication. From Privileged Exec mode, the operator can issue any Exec command or enter the Global Configuration mode. The command prompt shown at this level is:
Command Prompt: \$(Exec)# |
| Global Config Mode | This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port config, the Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:
Command Prompt: \$(Config)# |

From the Global Config mode, the operator may enter the following config modes:

- | | |
|------------------------------|---|
| VLAN Mode | This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:
Command Prompt: \$(VLAN)# |
| Interface Config Mode | Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface.
In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to |

the router interface configuration commands. The command prompt at this level is:

Command Prompt: \$(Interface <slot/port>)#

The resulting prompt for the interface configuration command entered in the Global Configuration mode is shown below:

\$(Config)# interface 2/1

\$(Interface 2/1)#

Line Config Mode

This mode allows the operator to configure the console interface. The operator may configure the interface from the directly connected console or the virtual terminal used with Telnet. The command prompt at this level is:

Command Prompt: \$(Line)#

Flow of Operation

This section captures the flow of operation for the CLI:

1. The operator logs into the CLI session and enters the User Exec mode. In the User Exec mode the \$(exec)> prompt is displayed on the screen.

The parsing process is initiated whenever the operator types a command and presses <ENTER>. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, command node A has the command "show arp brief" but the operator attempts to execute the command "show arpp brief" then the output message would be \$(exec)> show arpp brief^. *Invalid input detected at '^' marker*. If the operator has given an invalid input parameter in the command, then the message conveys to the operator an invalid input was detected. The layout of the output is depicted below:

```
(exec) #show arpp brief
          ^
%Invalid input detected at '^' marker.
```

FIGURE 2. Syntax Error Message

After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized a syntax error message will be displayed.

2. After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.
3. For mandatory parameters, the command tree extends till the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the call back function is associated with the node where the mandatory parameters are fetched. The call back function then takes care of the optional parameters.
4. Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.

“No” Form of a Command

“No” is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the “no” form. The behavior and the support details of the “no” form is captured as part of the mapping sheets. The mapping sheets are contained in the [Appendix A, “IS CLI Mapping”](#) section.

Support for “No” Form

Almost every configuration command has a “no” form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the “no shutdown interface” configuration command reverses the shutdown of an interface. Use the command without the keyword no to re-enable a disabled feature or to enable a feature that is disabled by default.

Behavior of Command Help (“?”)

The “no” form is treated as a specific form of an existing command and does not represent a new or distinct command. This implies that the behavior of the “?” and help text is the same for the “no” form:

- The help message is the same for all forms of the command. The help string may be augmented with details about the “no” form behavior.

- For the (no config interface?) and (no config inte?) cases of the “?”, the options displayed are identical to the case when the “no” token is not specified.

Chapter 8

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.
- Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.
- Copy commands transfers or saves configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

This chapter includes the following configuration types:

- System information and statistics commands
- Management commands
- Device configuration commands
- User account management commands
- Security commands
- System utilities

System Information and Statistics Commands

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	<code>show arp switch</code>
Mode	Privileged EXEC
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	Valid slot number and a valid port number.

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	<code>show eventlog</code>
Mode	Privileged EXEC
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 hardware

This command displays inventory information for the switch.

Format	<code>show hardware</code>
Mode	Privileged EXEC
Description	Text used to identify the product name of this switch.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.

show interface

This command displays a summary of statistics for a specific port or a count of all CPU traffic based upon the argument.

Format	<code>show interface {<slot/port> / switchport}</code>
---------------	--

Mode Privileged EXEC

The display parameters when the argument is '<slot/port>' is as follows:

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.

The display parameters when the argument is 'switchport' is as follows:

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

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

VLAN Entries Currently In Use The number of VLAN entries presently occupying the VLAN table.

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

show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Format	show interface ethernet {<slot/port> / switchport}
Mode	Privileged EXEC

The display parameters when the argument is '<slot/port>' is as follows:

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.

Tx 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 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.

The display parameters when the argument is 'switchport' is as follows:

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

Total 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 logging

This command displays the trap log maintained by the switch.

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

Format `show logging`

Mode `Privileged EXEC`

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.

show mac-addr-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 mac-addr-table [<macaddr> | all]`

Mode `Privileged EXEC`

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	<p>The status of this entry. The meanings of the values are:</p> <p>Static The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.</p> <p>Learned The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</p> <p>Management The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1 and is currently used when enabling VLANs for routing.</p> <p>Self The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).</p> <p>GMRP Learned The value of the corresponding was learned via GMRP and applies to Multicast.</p> <p>Other The value of the corresponding instance does not fall into one of the other categories.</p>

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	<code>show msglog</code>
Mode	Privileged EXEC
Message	The message that has been logged.

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

show running-config

This command is used to display the current setting of different protocol packages supported on switch. This command displays only those parameters, the values of which differ from default value. The output is displayed in the script format, which can be used to configure another switch with same configuration.

Format	<code>show running-config</code>
Mode	Privileged EXEC

show sysinfo

This command displays switch information.

Format	<code>show sysinfo</code>
Mode	Privileged EXEC
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.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for name, location and contact is from 1 to 31 alphanumeric characters.

Default	None
Format	<code>snmp-server {sysname <name> location <loc> contact <con>}</code>

Format	<code>Show classofservice dot1pmapping</code>
Mode	Privileged EXEC and User EXEC

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	<code>vlan port priority all <priority></code>
Mode	Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0-7

Default	0
Format	<code>vlan priority <priority></code>
Mode	Interface Config

LAG/Port-Channel (802.3ad) Commands

port-channel staticcapability

This command enables the support of port-channels (static link aggregations - LAGs) on the device. By default, the static capability for all port-channels is disabled.

Default	Disabled
Format	<code>port-channel staticcapability</code>
Mode	Global Config

no port-channel staticcapability

This command disables the support of static port-channels (link aggregations - LAGs) on the device.

Default	Disabled
----------------	----------

Format	<code>no port-channel staticcapability</code>
Mode	Global Config

show port-channel brief

This command displays the static capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

Format	<code>show port-channel brief</code>
Mode	Privileged EXEC and User EXEC
Static Capability	This field displays whether or not the device has static capability enabled.

For each port-channel the following information is displayed:

Name	This field displays the name of the port-channel.
Link State	This field indicates whether the link is up or down.
Mbr Ports	This field lists the ports that are members of this port-channel, in slot/port notation.
Active Ports	This field lists the ports that are actively participating in this port-channel.

Management Commands

These commands manage the switch and show current management settings.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. 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	300
Format	<code>bridge aging-time <10-1,000,000> [fdbid all]</code>
Mode	Global Config

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.

no bridge aging-time

This command sets the forwarding database address aging timeout to 300 seconds. 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.

Format no bridge aging-time [fdbid / all]

Mode Global Config

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.

mtu

This command sets the maximum transmission unit (MTU) size (in bytes) for physical and port-channel (LAG) interfaces. For the standard implementation, the range of <mtusize> is a valid integer between 1522-9216.

Default 1522

Format mtu <1522-9216>

Mode Interface Config

no mtu

This command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

Format no mtu

Mode Interface 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	Enabled
Format	network javamode
Mode	Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

Format	no network javamode
Mode	Privileged EXEC

network mac-address

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	network mac-address <macaddr>
Mode	Privileged EXEC

network mac-type

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

Default	burnedin
Format	network mac-type {local burnedin}

Mode Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format no network mac-type

Mode Privileged EXEC

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 network parms <ipaddr> <netmask> [<gateway>]

Mode Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value change is effective immediately.

Default None

Format 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.

Mode Privileged EXEC

remotecon maxsessions

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

Default 5

Format remotecon maxsessions <0-5>

Mode Privileged EXEC

no remotecon maxsessions

This command sets the maximum number of remote connection sessions that can be established to the default value.

Default	5
Format	no remotecon maxsessions
Mode	Privileged EXEC

remotecon timeout

This command sets the remote connection 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	remotecon timeout <0-160>
Mode	Privileged EXEC

no remotecon timeout

This command sets the remote connection session timeout value, in minutes, to the default.

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	no remotecon timeout
Mode	Privileged EXEC

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 `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`

Mode `Line Config`

no serial baudrate

This command sets the communication rate of the terminal interface to 9600.

Format `no serial baudrate`

Mode `Line 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 `serial timeout <0 - 160>`

Mode `Line Config`

no serial timeout

This command sets the maximum connect time (in minutes) without console activity to 5.

Format `no serial timeout`

Mode `Line Config`

set prompt

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

Format `set prompt <prompt string>`

Mode `Privileged EXEC`

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	<code>all</code>
Format	<code>show forwardingdb agetime [fdbid / all]</code>
Mode	Privileged EXEC
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.

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format	<code>show network</code>
Mode	Privileged EXEC and User EXEC
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
Burned In MAC Address	The burned in 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 burned in or the Locally Administered address. The factory default is to use the burned in MAC address.

Network Configuration Protocol Current Indicates which network protocol is being used. The options are bootp | dhcp | none.

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 disabled.

Management VLAN ID Specifies the management VLAN ID.

show remotecon

This command displays telnet settings.

Format `show remotecon`

Mode `Privileged EXEC and User EXEC`

Remote Connection Login Timeout (minutes) This object indicates the number of minutes a remote connection 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 Remote Connection Sessions This object indicates the number of simultaneous remote connection 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.

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Mode	Privileged EXEC and User EXEC
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. 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.

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	<code>show snmpcommunity</code>
Mode	Privileged EXEC
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.

Status

The status of this community access entry.

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`

Mode

`Privileged EXEC`

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.

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	<code>show trapflags</code>
Mode	Privileged EXEC
Authentication Flag	May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent. Multiple Users Flag.
Multiple Users Flag	May be enabled or disabled. 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. The factory default is enabled. Indicates whether spanning tree traps will be sent.
Broadcast Storm Flag	May be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps will be sent.
DVMRP Traps	May be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps will be sent.
OSPF Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.
PIM Traps	May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.

snmp-server community

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	<code>snmp-server community <name></code>
Mode	Global Config

no snmp-server community

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

Format	<code>no snmp-server community <name></code>
Mode	Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default	0.0.0.0
Format	<code>snmp-server community ipaddr <ipaddr> <name></code>
Mode	Global Config

no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to **0.0.0.0**. The name is the applicable community name.

Format	<code>no snmp-server community ipaddr <name></code>
Mode	Global Config

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default	0.0.0.0
Format	<code>snmp-server community ipmask <ipmask> <name></code>
Mode	Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to **0.0.0.0**. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Format	<code>no snmp-server community ipmask <name></code>
Mode	Global Config

snmp-server community mode

This command activates 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	<code>snmp-server community mode <name></code>
Mode	Global Config

no snmp-server community mode

This command deactivates an SNMP community. 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.

Format `no snmp-server community mode <name>`
Mode `Global Config`

snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format `snmp-server community ro <name>`
Mode `Global Config`

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format `snmp-server community rw <name>`
Mode `Global Config`

snmp-server enable traps

This command enables the Authentication Flag.

Default `Enabled`
Format `snmp-server enable traps`
Mode `Global Config`

no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`
Mode `Global Config`

snmp-server enable traps bcstorm

This command enables 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.

Default	Enabled
Format	snmp-server enable traps bcaststorm
Mode	Global Config

no snmp-server enable traps bcaststorm

This command 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.

Format	no snmp-server enable traps bcaststorm
Mode	Global Config

snmp-server enable traps linkmode

This command enables 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 ‘snmp trap link-status’ command).

Default	Enabled
Format	snmp-server enable traps linkmode
Mode	Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format	no snmp-server enable traps linkmode
Mode	Global Config

snmp-server enable traps multiusers

This command enables 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	Enabled
Format	snmp-server enable traps multiusers
Mode	Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format	<code>no snmp-server enable traps multiusers</code>
Mode	Global Config

snmp-server enable traps stpmode

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

Default	Enabled
Format	<code>snmp-server enable traps stpmode</code>
Mode	Global Config

no snmp-server enable traps stpmode

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

Format	<code>no snmp-server enable traps stpmode</code>
Mode	Global Config

snmptrap

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	<code>snmptrap <name> <ipaddr></code>
Mode	Global Config

no snmptrap

This command deletes trap receivers for a community.

Format	<code>no snmptrap <name> <ipaddr></code>
Mode	Global 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 `snmptrap ipaddr <name> <ipaddrold> <ipaddrnew>`

Mode Global 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 `snmptrap mode <name> <ipaddr>`

Mode Global Config

no snmptrap mode

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

Format `no snmptrap mode <name> <ipaddr>`

Mode Global Config

telnet

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 Enabled

Format `telnet`

Mode Privileged EXEC

no telnet

This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

Format	<code>no telnet</code>
Mode	Privileged EXEC

HTTP Commands

ip http secure-port

This command is used to set the sslt port where port can be 1-65535 and the default is port 443.

Default	443
Format	<code>ip http secure-port <portid></code>
Mode	Privileged EXEC

no ip http secure-port

This command is used to reset the sslt port to the default value.

Format	<code>no ip http secure-port</code>
Mode	Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default	SSL3 and TLS1
Format	<code>ip http secure-protocol [SSL3] [TLS1]</code>
Mode	Privileged EXEC

no ip http secure-protocol

This command is used to remove protocol levels (versions) for secure HTTP.

Format	<code>no ip http secure-protocol [SSL3] [TLS1]</code>
---------------	---

Mode Privileged EXEC

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default Disabled
Format ip http secure-server
Mode Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format ip http secure-server
Mode Privileged EXEC

ip http server

This command enables 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 enabled
Format ip http server
Mode Privileged EXEC

no ip http server

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

Default enabled
Format no ip http server
Mode Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format	<code>show ip http</code>
Mode	Privileged EXEC
Secure-Server Administrative Mode	This field indicates whether the administrative mode of secure HTTP is enabled or disabled.
Secure Protocol Level	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Secure Port	This field specifies the port configured for SSLT.
HTTP Mode	This field indicates whether the HTTP mode is enabled or disabled.

Secure Shell (SSH) Commands

ip ssh

This command is used to enable SSH.

Default	Disabled
Format	<code>ip ssh</code>
Mode	Privileged EXEC

no ip ssh

This command is used to disable SSH.

Format	<code>no ip ssh</code>
Mode	Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	1 and 2
----------------	---------

Format	<code>ip ssh protocol [1] [2]</code>
Mode	Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format	<code>show ip ssh</code>
Mode	Privileged EXEC
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
Connections	This field specifies the current ssh connections.

Device Configuration Commands

addport

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

Note: Before adding a port to a port-channel, set the physical mode of the port. See 'speed' command.

Format	<code>addport <logical slot/port></code>
Mode	Interface Config

auto-negotiate

This command enables automatic negotiation on a port. The default value is enable.

Format	<code>auto-negotiate</code>
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Format	<code>no auto-negotiate</code>
Mode	Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports. The default value is enable.

Format	<code>auto-negotiate all</code>
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	<code>no auto-negotiate all</code>
Mode	Global Config

delete interface

This command deletes an existing port-channel (LAG) from the configuration. The interface is a logical slot and port for a configured port-channel. The `all` option removes all configured port-channels (LAGs).

Format	<code>delete interface {<logical slot/port> all}</code>
Mode	Interface Config

deleteport

This command deletes the port from the port-channel (LAG). The interface is a logical slot and port number of a configured port-channel.

Format	<code>deleteport <logical slot/port></code>
Mode	Interface Config

no monitor session mode

This command sets the monitor session (port monitoring) mode to disable.

Format	<code>no monitor session mode</code>
Mode	Global Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

Default	Disabled
Format	<code>port lacpmode</code>
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	<code>no port lacpmode</code>
Mode	Interface Config

port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	<code>port lacpmode all</code>
Mode	Global Config

no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	<code>no port lacpmode all</code>
Mode	Global Config

port-channel

This command configures a new port-channel (LAG) and generates a logical slot and port number for it. Display this number using the “show port-channel”.

Note: Before including a port in a port-channel, set the port physical mode. See ‘speed’ command.

Format `port-channel <name>`
Mode `Global Config`

port-channel adminmode

This command enables a port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format `port-channel adminmode {<logical slot/port> | all}`
Mode `Global Config`

no port-channel adminmode

This command disables a port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format `no port-channel adminmode {<logical slot/port> | all}`
Mode `Global Config`

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Default `Enabled`
Format `port-channel linktrap {<logical slot/port> | all}`
Mode `Global Config`

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format `no port-channel linktrap {<logical slot/port> | all}`

Mode GlobalConfig

port-channel name

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

Format port-channel name {<logical slot/port> | all} <name>

Mode Global Config

protocol group

This command attaches a <vlanid> 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 protocol group <groupid> <vlanid>

Mode VLAN database

no protocol group

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

Format no protocol group <groupid> <vlanid>

Mode VLAN database

protocol vlan group

This command adds the physical <slot/port> interface to the protocol-based VLAN identified by <groupid>. 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 protocol vlan group <groupid>

Format `set garp timer join <10-100>`
Mode `Interface Config`

no set garp timer join

This command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Format `no set garp timer join`
Mode `Interface Config`

set garp timer join all

This command sets the GVRP join time for all ports 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 `set garp timer join all <10-100>`
Mode `Global Config`

no set garp timer join all

This command sets the GVRP join time for all ports and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Format `no set garp timer join all`
Mode `Global Config`

set garp timer leave

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	<code>set garp timer leave <20-600></code>
Mode	Interface Config

no set garp timer leave

This command sets the GVRP leave time per port to 60 centiseconds (0.6 seconds).

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

Format	<code>no set garp timer leave</code>
Mode	Interface Config

set garp timer leave all

This command sets the GVRP leave time for all ports. 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	<code>set garp timer leave all <20-600></code>
Mode	Global Config

no set garp timer leave all

This command sets the GVRP leave time for all ports to the default 60 centiseconds (0.6 seconds).

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

Format	<code>no set garp timer leave all</code>
Mode	Global Config

set garp timer leaveall

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	<code>set garp timer leaveall <200-6000></code>
Mode	Interface Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated per port to 1000 centiseconds (10 seconds).

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

Format	<code>no set garp timer leaveall</code>
Mode	Interface Config

set garp timer leaveall all

This command sets how frequently Leave All PDUs are generated for all ports. 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	<code>set garp timer leaveall all <200-6000></code>
Mode	Global Config

no set garp timer leaveall all

This command sets how frequently Leave All PDUs are generated for all ports to 1000 centiseconds (10 seconds).

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

Format `no set garp timer leaveall all`
Mode `Global Config`

set gmrp adminmode

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

Format `set gmrp adminmode`
Mode `Privileged EXEC`

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format `no set gmrp adminmode`
Mode `Privileged EXEC`

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default `Disabled`
Format `set gmrp interfacemode`
Mode `Interface Config`

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format `no set gmrp interfacemode`
Mode `Interface Config`

set gmrp interfacemode all

This command enables GARP Multicast Registration Protocol on all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	Disabled
Format	<code>set gmrp interfacemode all</code>
Mode	Global Config

no set gmrp interfacemode all

This command disables GARP Multicast Registration Protocol on a selected interface.

Format	<code>no set gmrp interfacemode all</code>
Mode	Global Config

set gvrp adminmode

This command enables GVRP.

Default	Disabled
Format	<code>set gvrp adminmode</code>
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	<code>no set gvrp adminmode</code>
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Default	Disabled
Format	<code>set gvrp interfacemode</code>

no set igmp

This command disables IGMP Snooping on the system.

Format	<code>no set igmp</code>
Mode	<code>Global Config</code>

set igmp

This command enables IGMP Snooping on a selected interface. If an interface which has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or port-channel (LAG) membership is removed from an interface that has IGMP Snooping enabled.

Default	Disabled
Format	<code>set igmp</code>
Mode	<code>Interface Config</code>

no set igmp

This command disables IGMP Snooping on a selected interface.

Format	<code>no set igmp</code>
Mode	<code>Interface Config</code>

set igmp 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	<code>set igmp groupmembershipinterval <1-3600></code>
Mode	<code>Global Config</code>

no set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system to 260 seconds.

Format `no set igmp groupmembershipinterval`
Mode `Global Config`

set igmp interfacemode all

This command enables IGMP Snooping on all interfaces. If an interface which has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or port-channel (LAG) membership is removed from an interface that has IGMP Snooping enabled.

Default `Disabled`
Format `set igmp interfacemode all`
Mode `Global Config`

no set igmp interfacemode all

This command disables IGMP Snooping on all interfaces.

Format `no set igmp interfacemode all`
Mode `Global Config`

set igmp 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 `set igmp maxresponse <1-3600>`
Mode `Global Config`

no set igmp maxresponse

This command sets the IGMP Maximum Response time on the system to 10 seconds.

Format `no set igmp maxresponse`
Mode `Global Config`

set igmp mcrtxpiretime

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	<code>set igmp mcrtxpiretime <0-3600></code>
Mode	Global Config

no set igmp mcrtxpiretime

This command sets the Multicast Router Present Expiration time on the system to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

Format	<code>no set igmp mcrtxpiretime</code>
Mode	Global Config

show garp

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

Format	<code>show garp</code>
Mode	Privileged EXEC and User EXEC
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 gmrp configuration

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

Format	<code>show gmrp configuration {<slot/port> all}</code>
Mode	Privileged EXEC and User EXEC
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 unregister 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 $1.5 * \text{LeaveAllTime}$. 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.

show gvrp configuration

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

Format `show gvrp configuration {<slot/port> | all}`

Mode Privileged EXEC and User EXEC

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 unregister 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.

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`

Mode

`Privileged EXEC`

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 IGMP 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.

show mac-address-table gmrp

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

Format	<code>show mac-address-table gmrp</code>
Mode	Privileged EXEC
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 mac-address-table igmpsnooping

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

Format	<code>show mac-address-table igmpsnooping</code>
Mode	Privileged EXEC
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 mac-address-table multicast

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	<code>show mac-address-table multicast [<macaddr> all]</code>
Mode	Privileged EXEC
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 mac-address-table static

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	<code>show mac-address-table static {<macaddr> <vlanid> all}</code>
Mode	Privileged EXEC
MAC Address	Is the MAC Address of the static MAC filter entry.
VLAN ID	Is 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).

show mac-address-table staticfiltering

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

Format	<code>show mac-address-table staticfiltering</code>
Mode	Privileged EXEC
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 mac-address-table stats

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

Format	<code>show mac-address-table stats</code>
Mode	Privileged EXEC
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 monitor

This command displays the Port monitoring information for the system.

Format	<code>show monitor</code>
Mode	Privileged EXEC
Port Monitor Mode	indicates whether the Port Monitoring 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.
Monitored Port slot/port	is the slot/port that is configured as the monitored port. If this value has not been configured, 'Not Configured' will be displayed.

show port

This command displays port information.

Format	<code>show port {<slot/port> all}</code>
Mode	Privileged EXEC
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 port-channel (LAG). Probe - this port is a probe port.
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. 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.

show port protocol

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

Format	<code>show port protocol {<groupid> all}</code>
Mode	Privileged EXEC
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.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format	<code>show port-channel {<logical slot/port> all}</code>
Mode	Privileged EXEC
Logical slot/port	The logical slot and the logical port.

Name	The name of this port-channel (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. 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 port-channel (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 port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Port Speed	Speed of the port-channel port.
Type	This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are Static, indicating that the port-channel is statically maintained; and Dynamic, indicating that the port-channel is dynamically maintained.
Active Ports	This field lists the ports that are actively participating in the port-channel (LAG).

show storm-control

This command displays switch configuration information.

Format	<code>show storm-control</code>
Mode	Privileged EXEC
Broadcast Storm Recovery Mode	May be enabled or disabled. The factory default is disabled.
802.3x Flow Control Mode	May be enabled or disabled. The factory default is disabled.

show vlan

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

Format	<code>show vlan <vlanid></code> , where the ID is a valid VLAN identification number
Mode	Privileged EXEC and User EXEC
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	Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
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.

show vlan brief

This command displays a list of all configured VLANs.

Format	<code>show vlan brief</code>
Mode	Privileged EXEC and User EXEC
VLAN ID	There is a VLAN Identifier (vlanid) 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	Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format	<code>show vlan port {<slot/port> all}</code>
Mode	Privileged EXEC and User EXEC
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. 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

May be enabled or disabled.

Default Priority

The 802.1p priority assigned to tagged packets arriving on the port.

shutdown

This command disables a port.

Default	<code>Enabled</code>
Format	<code>shutdown</code>
Mode	<code>Interface Config</code>

no shutdown

This command enables a port.

Format	<code>no shutdown</code>
Mode	<code>Interface Config</code>

shutdown all

This command disables all ports.

Default	<code>Enabled</code>
Format	<code>shutdown all</code>
Mode	<code>Global Config</code>

no shutdown all

This command enables all ports.

Format	<code>no shutdown all</code>
Mode	Global Config

snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command.

Format	<code>snmp trap link-status</code>
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command).

Format	<code>no snmp trap link-status</code>
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format	<code>snmp trap link-status all</code>
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format `no snmp trap link-status all`
Mode `Global Config`

spanning-tree

This command sets the STP mode for a specific port-channel (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 port-channel. The **all** option sets all configured port-channels (LAGs) with the same option.

Format `spanning-tree {<logical slot/port> | all} {off | 802.1d | fast}`
Mode `Global Config`

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

spanning-tree bpdumigrationcheck

This command enables BPDU migration check on a given interface. The **all** option enables BPDU migration check on all interfaces.

Format `spanning-tree bpdumigrationcheck {<slot/port> | all}`
Mode `Global Config`

no spanning-tree bpdumigrationcheck

This command disables BPDU migration check on a given interface. The **all** option disables BPDU migration check on all interfaces.

Format `no spanning-tree bpdumigrationcheck {<slot/port> | all}`
Mode `Global Config`

speed

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

Format `speed {{100 | 10} {half-duplex | full-duplex} | 1000 full-duplex}`
Mode

Interface Config

Acceptable values are:

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

speed all

This command sets the speed and duplex setting for all interfaces.

Format `speed all {{100 | 10} {half-duplex | full-duplex} | 1000 full-duplex}`
Mode Global Config

Acceptable values are:

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

storm-control broadcast

This command enables 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 8-1. Broadcast Storm Recovery Thresholds

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

Format `switchconfig storm-control broadcast`

Mode Global Covnfig

no storm-control broadcast

This command disables broadcast storm recovery mode.

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 8-2. Broadcast Storm Recovery Thresholds

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

Format `no switchconfig storm-control broadcast`

Mode Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch.

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

Default	Disabled
Format	storm-control flowcontrol
Mode	Global Config

no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

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

Format	no storm-control flowcontrol
Mode	Global Config

vlan

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	vlan <2-4094>
Mode	VLAN database

no vlan

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	no vlan <2-4094>
Mode	VLAN database

vlan 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.

Default	<code>Admit All</code>
Format	<code>vlan acceptframe {vlanonly all}</code>
Mode	<code>Interface Config</code>

no vlan acceptframe

This command sets the frame acceptance mode per interface to **Admit All**. 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.

Format	<code>vlan acceptframe {vlanonly all}</code>
Mode	<code>Interface Config</code>

vlan ingressfilter

This command enables 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	<code>Disabled</code>
Format	<code>vlan ingressfilter</code>
Mode	<code>Interface Config</code>

no vlan ingressfilter

This command 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.

Format	<code>no vlan ingressfilter</code>
Mode	<code>Interface Config</code>

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 `vlan makestatic <2-4094>`
Mode `VLAN database`

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 `vlan name <2-4094> <name>`
Mode `VLAN database`

no vlan name

This command sets the name of a VLAN to a blank string. The VLAN ID is a valid VLAN identification number. ID range is 1-4094.

Format `no vlan name <2-4094>`
Mode `VLAN database`

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.

Format `vlan participation {exclude | include | auto} <1-4094>`
Mode `Interface Config`

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.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format	<code>vlan participation all {exclude include auto} <1-4094></code>
Mode	Global Config

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.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. 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.

Default	Admit All
Format	<code>vlan port acceptframe all {vlanonly all}</code>
Mode	Global Config

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to **Admit All**. 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.

Format	<code>no vlan port acceptframe all {vlanonly all}</code>
Mode	Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. 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	Disabled
Format	<code>vlan port ingressfilter all</code>
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. 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.

Format	<code>no vlan port ingressfilter all</code>
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	<code>vlan port pvid all <1-4094></code>
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format `no vlan port pvid all <1-4094>`
Mode `Global Config`

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. 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.

Format `vlan port tagging all <1-4094>`
Mode `Global Config`

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan port tagging all <1-4094>`
Mode `Global Config`

vlan protocol group

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 `vlan protocol group <groupname>`
Mode `Global Config`

vlan protocol group add protocol

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 `vlan protocol group add protocol <groupid> <protocol>`
Mode `Global Config`

no vlan protocol group add protocol

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.

Format `no vlan protocol group add protocol <groupid> <protocol>`
Mode `Global Config`

vlan protocol group remove

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

Format `vlan protocol group remove <groupid>`
Mode `Global Config`

vlan pvid

This command changes the VLAN ID per interface.

Default `1`
Format `vlan pvid <1-4094>`
Mode `Interface Config`

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format `no vlan pvid <1-4094>`
Mode `Interface Config`

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. 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.

Format `vlan tagging <1-4094>`
Mode `Interface Config`

no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan tagging <1-4094>`
Mode `Interface Config`

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.
- Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Format `show spanning-tree [brief]`
Mode `Privileged EXEC and User EXEC`
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	
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.

When the “brief” optional parameter is included, this command displays spanning tree settings for the bridge. In this case, the following details are displayed.

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)

show spanning-tree interface

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. The following details are displayed on execution of the command.

Format	show spanning-tree interface <slot/port>
Mode	Privileged EXEC and User EXEC
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.

show spanning-tree 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. The following details are displayed.

Format show spanning-tree mst detailed <mstid>

Mode Privileged EXEC and User EXEC

MST Instance ID

MST Bridge Priority

Time Since Topology Change 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 spanning-tree 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 spanning-tree mst port detailed <mstid> <slot/port>
Mode	Privileged EXEC and User EXEC
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

If 0 (defined as the default CIST ID) is passed as the <mstid>, then 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. In this case, the following are displayed.

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.

show spanning-tree 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.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Format	show spanning-tree mst port summary <mstid> {<slot/port> all}
Mode	Privileged EXEC and User EXEC
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 spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format	show spanning-tree mst summary
Mode	Privileged EXEC and User EXEC
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 spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format	show spanning-tree summary
Mode	Privileged EXEC and User EXEC
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

show spanning-tree vlan

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

Format	show spanning-tree vlan <vlanid>
Mode	Privileged EXEC and User EXEC
VLAN Identifier	
Associated Instance	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	Disabled
Format	spanning-tree
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	no spanning-tree
Mode	Global Config

spanning-tree 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	spanning-tree configuration name <name>
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	no spanning-tree configuration name
Mode	Global Config

spanning-tree configuration revision

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

Default	0
Format	spanning-tree configuration revision <0-65535>
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, i.e. 0.

Format	no spanning-tree configuration revision
Mode	Global Config

spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format	spanning-tree edgeport
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	no spanning-tree edgeport
Mode	Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol 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	spanning-tree forceversion <802.1d 802.1w 802.1s>
Mode	Global Config

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value, i.e. 802.1s.

Format	no spanning-tree forceversion
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in 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	spanning-tree forward-time <4-30>
Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, i.e. 15.

Format	no spanning-tree forward-time
Mode	Global Config

spanning-tree hello-time

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	spanning-tree hello-time <1-10>
Mode	Global Config

no spanning-tree hello-time

This command sets the Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

Format	no spanning-tree hello-time
Mode	Global Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in 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	spanning-tree max-age <6-40>
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, i.e. 20.

Format	no spanning-tree max-age
Mode	Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. 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.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	cost: auto
port-priority	128
Format	spanning-tree mst <mstid> {cost {<1-200000000> auto} port-priority <0-240>}
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

Format no spanning-tree mst <mstid> {cost | port-priority}
Mode Interface Config

spanning-tree mst instance

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 the 7200 Series L2 Switch is 4.

Format spanning-tree mst instance <mstid>
Mode Global Config

no spanning-tree mst instance

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 no spanning-tree mst instance <mstid>
Mode Global Config

spanning-tree 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.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again 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 spanning-tree mst priority <mstid> <0-61440>
Mode Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value, i.e. 32768. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

Format spanning-tree mst priority <mstid>

Mode Global Config

spanning-tree mst vlan

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 <vlanid> corresponds to an existing VLAN ID.

Format spanning-tree mst vlan <mstid> <vlanid>

Mode Global Config

no spanning-tree mst vlan

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 <vlanid> corresponds to an existing VLAN ID.

Format no spanning-tree mst vlan <mstid> <vlanid>

Mode Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default Disabled

Format spanning-tree port mode

Mode Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format	no spanning-tree port mode
Mode	Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	Disabled
Format	spanning-tree port mode all
Mode	Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format	no spanning-tree port mode all
Mode	Global Config

User Account Management Commands

These commands manage user accounts.

disconnect

This command closes a telnet session.

Format	<code>disconnect {<sessionID> all}</code>
Mode	Privileged EXEC

show loginsession

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

Format	<code>show loginsession</code>
---------------	--------------------------------

Mode Privileged EXEC

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.

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 `show users`

Mode Privileged EXEC

User Name 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 eight 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 five Read Only users.

SNMPv3 AccessMode 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.

SNMPv3 Authentication This field displays the authentication protocol to be used for the specified login user.

SNMPv3 Encryption This field displays the encryption protocol to be used for the specified login user.

users name

This command adds a new user (account) if space permits. The account <username> can be up to eight characters in length. The name may be comprised of alphanumeric characters as well as the dash ('-') and underscore ('_'). The <username> is not case-sensitive.

Six user names can be defined.

Format `users name <username>`

Mode `Global Config`

no users name

This command removes an operator.

Format `no users name <username>`

Mode `Global Config`

Note: The admin user account cannot be deleted.

users passwd

This command changes the password of an existing operator. User password should not be more than eight characters in length. If a user is authorized for authentication or encryption is enabled, password must be eight alphanumeric characters in length. The username 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 `No Password`

Format `users passwd <username>`

Mode `Global Config`

no users passwd

This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

Format	<code>no users passwd <username></code>
Mode	Global 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 <username> is the login user name for which the specified access mode will apply.

Default	<code>readwrite</code> for admin user; <code>readonly</code> for all other users
Format	<code>users snmpv3 accessmode <username> {readonly readwrite}</code>
Mode	Global Config

no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified login user as **readwrite** for admin user; **readonly** for all other users. The <username> is the login user name for which the specified access mode will apply.

Format	<code>no users snmpv3 accessmode <username></code>
Mode	Global 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 <username> is the login user name for which the specified authentication protocol will be used.

Default	no authentication
Format	<code>users snmpv3 authentication <username> {none md5 sha}</code>
Mode	Global Config

no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified login user to **none**. The <username> is the login user name for which the specified authentication protocol will be used.

Format `users snmpv3 authentication <username>`
Mode `Global 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 <username> is the login user name for which the specified encryption protocol will be used.

Default `no encryption`
Format `users snmpv3 encryption <username> {none | des [key]}`
Mode `Global Config`

no users snmpv3 encryption

This command sets the encryption protocol to **none**. The <username> is the login user name for which the specified encryption protocol will be used.

Format `no users snmpv3 encryption <username>`
Mode `Global Config`

Security Commands

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

authentication login

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.

When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set 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.

Format `authentication login <listname> [method1 [method2 [method3]]]`

Mode `Global Config`

no authentication login

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 `no authentication login <listname>`

Mode `Global Config`

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format	clear dot1x statistics { <slot/port> all }
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	clear radius statistics
Mode	Privileged EXEC

dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden 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	dot1x defaultlogin <listname>
Mode	Global Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format	dot1x initialize <slot/port>
Mode	Privileged EXEC

dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The <user> parameter must be a configured user and the <listname> parameter must be a configured authentication login list.

Format dot1x login <user> <listname>
Mode Global Config

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The <count> value must be in the range 1 - 10.

Default 2
Format dot1x max-req <count>
Mode Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant to the default value, i.e. 2.

Format no dot1x max-req
Mode Interface Config

dot1x port-control

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

- **force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
- **force-authorized:** 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 dot1x port-control {force-unauthorized | force-authorized | auto}
Mode Interface Config

no dot1x port-control

This command sets the authentication mode to be used on the specified port to 'auto'.

Format	no dot1x port-control
Mode	Interface Config

dot1x port-control All

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

- **force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
- **force-authorized:** 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	dot1x port-control all {force-unauthorized force-authorized auto}
Mode	Global Config

no dot1x port-control All

This command sets the authentication mode to be used on all ports to 'auto'.

Format	no dot1x port-control all
Mode	Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format	dot1x re-authenticate <slot/port>
Mode	Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default	Disabled
Format	dot1x re-authentication
Mode	Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format	no dot1x re-authentication
Mode	Interface Config

dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	Disabled
Format	dot1x system-auth-control
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	no dot1x system-auth-control
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.

reauth-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

quiet-period: 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 must be a value in the range 0 - 65535.

tx-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

supp-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

server-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	reauth-period: 3600 seconds quiet-period: 60 seconds tx-period: 30 seconds supp-timeout: 30 seconds server-timeout: 30 seconds
Format	dot1x timeout { {reauth-period <seconds>} {quiet-period <seconds>} {tx-period <seconds>} {supp-timeout <seconds>} {server-timeout <seconds>} }
Mode	Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format	no dot1x timeout { reauth-period quiet-period tx-period supp-timeout server-timeout }
Mode	Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <user> parameter must be a configured user.

Format dot1x user <user> {<slot/port> | all}

Mode Global Config

no dot1x user

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

Format no dot1x user <user> {<slot/port> | all}

Mode Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default Disabled

Format radius accounting mode

Mode Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format no radius accounting mode

Mode Global Config

radius server host

This command is used to configure the RADIUS authentication and accounting server.

If the 'auth' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional <port> parameter is used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the 'acct' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional <port> parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

Format radius server host {auth | acct} <ipaddr> [<port>]
Mode Global Config

no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The <ipaddr> parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Format no radius server host {auth | acct} <ipaddress>
Mode Global Config

radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Format	radius server key {auth acct} <ipaddr>
Mode	Global Config

radius server msgauth

This command enables the message authenticator attribute for a specified server.

Default	radius server msgauth <ipaddr>
Mode	Global Config

radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format	radius server primary <ipaddr>
Mode	Global Config

radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Default	10
----------------	----

Format `radius server retransmit <retries>`
Mode `Global Config`

no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

Format `no radius server retransmit`
Mode `Global Config`

radius server 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 to 30.

Default `6`
Format `radius server timeout <seconds>`
Mode `Global Config`

no radius server 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, to the default value, i.e. 6.

Format `no radius server timeout`
Mode `Global Config`

show accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format `show accounting [statistics <ipaddr>]`
Mode `Privileged EXEC`

If the optional token 'statistics <ipaddr>' is not included, then only the accounting mode and the RADIUS accounting server details are displayed.

Mode	Enabled or disabled
IP Address	The configured IP address of the RADIUS accounting server
Port	The port in use by the RADIUS accounting server
Secret Configured	Yes or No

If the optional token 'statistics <ipaddr>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Accounting Server IP Address	IP Address of the configured RADIUS accounting server
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 the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed 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 containing 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 types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

show authentication

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

Format	<code>show authentication</code>
Mode	Privileged EXEC
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 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	<code>show authentication users <listname></code>
Mode	Privileged EXEC
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

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format	<code>show dot1x [{summary {<slot/port> all}} {detail <slot/port>} {statistics <slot/port>}]</code>
Mode	Privileged EXEC

If none of the optional parameters are used, the global dot1x configuration summary is displayed.

Administrative mode	Indicates whether authentication control on the switch is enabled or disabled. If the optional parameter 'summary {<slot/port> all}' is used, the dot1x configuration for the specified port or all ports are displayed.
Port	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized / force-authorized / auto
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized / unauthorized
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port

If the optional parameter 'detail <slot/port>' is used, the detailed dot1x configuration for the specified port are displayed.

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.

If the optional parameter 'statistics <slot/port>' is used, the dot1x statistics for the specified port are displayed.

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.

show dot1x users

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

Format	show dot1x users <slot/port>
Mode	Privileged EXEC
User	Users configured locally to have access to the specified port.

show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items will be displayed.

Format	show radius [servers]
Mode	Privileged EXEC

Primary Server IP Address Indicates the configured server currently in use for authentication

Number of configured servers The configured IP address of the authentication server

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 re-transmissions

Accounting Mode Yes or No

If the optional token 'servers' is included, the following information regarding the configured RADIUS servers is displayed.

IP Address IP Address of the configured RADIUS server

Port The port in use by this server

Type Primary or secondary

Secret Configured Yes / No

show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format show radius statistics [ipaddr]

Mode Privileged EXEC

If ip address is not specified than only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

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

Server IP Address

Round Trip Time The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission	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, which were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which 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 types, 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 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	<code>show users authentication</code>
Mode	Privileged EXEC
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.

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	<code>users defaultlogin <listname></code>
Mode	Global 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.

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

Format	<code>users login <user> <listname></code>
Mode	Global Config

System Utilities

This section describes system utilities.

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	<code>clear config</code>
---------------	---------------------------

Mode Privileged EXEC

clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire switch based upon the argument.

Format `clear counters [{<slot/port> | all}]`

Mode Privileged EXEC

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`

Mode Privileged EXEC

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`

Mode Privileged EXEC

clear port-channel

This command clears all port-channels (LAGs).

Format `clear port-channel`

Mode Privileged EXEC

clear traplog

This command clears the trap log.

Format `clear traplog`

Mode Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format	<code>clear vlan</code>
Mode	Privileged EXEC

copy

This command uploads and downloads to/from the switch. Local URLs can be specified using tftp or xmodem. The following can be specified as the source file for uploading from the switch: startup config (*nvr_{am}:startup-config*), error log (*nvr_{am}:errorlog*), message log (*nvr_{am}:msglog*) and trap log (*nvr_{am}:traplog*). A URL is specified for the destination.

The command can also be used to download the startup config or code image by specifying the source as a URL and destination as *nvr_{am}:startup-config* or *.system:image* respectively.

The command can be used to save the running config to nvr_{am} by specifying the source as *system:running-config* and the destination as *nvr_{am}:startup-config*

The command can also be used to download ssh key files as *nvr_{am}:sshkey-rsa*, *nvr_{am}:sshkey-rsa2*, and *nvr_{am}:sshkey-dsa* and http secure-server certificates as *nvr_{am}:sslpem-root*, *nvr_{am}:sslpem-server*, *nvr_{am}:sslpem-dhweak*, and *nvr_{am}:sslpem-dhstrong*.

Default	none
Format	<code>copy nvr_{am}:startup-config <url></code> <code>copy nvr_{am}:errorlog <url></code> <code>copy nvr_{am}:msglog <url></code> <code>copy nvr_{am}:traplog <url></code> <code>copy <url> nvr_{am}:startup-config</code> <code>copy <url> system:image</code> <code>copy system:running-config nvr_{am}:startup-config</code> <code>copy <url> nvr_{am}:sslpem-root</code> <code>copy <url> nvr_{am}:sslpem-server</code> <code>copy <url> nvr_{am}:sslpem-dhweak</code> <code>copy <url> nvr_{am}:sslpem-dhstrong</code> <code>copy <url> nvr_{am}:sshkey-rsa1</code> <code>copy <url> nvr_{am}:sshkey-rsa2</code>

Mode copy <url> nvram:sshkey-dsa
Privileged EXEC

logout

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

Note: Save configuration changes before logging out.

Format logout
Mode Privileged EXEC

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 *7200 Series L2 Switch 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>
Mode Privileged EXEC and User EXEC

reload

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 reload
Mode Privileged EXEC

Chapter 9

DHCP Server Commands

DHCP Server Configuration Commands

These commands configure the DHCP Server parameters and address pools.

client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format.

Default	None
Format	<code>client-identifier <uniqueidentifier></code>
Mode	DHCP Pool Config Mode

no client-identifier

This command deletes the client identifier.

Format	<code>no client-identifier</code>
Mode	DHCP Pool Config Mode

client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	None
Format	<code>client-name <name></code>
Mode	DHCP Pool Config Mode

no client-name

This command removes the client name.

Format	<code>no client-name</code>
Mode	DHCP Pool Config Mode

default-router

This command specifies the default router list for a DHCP client. {address1, address2... address8} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	None
Format	<code>default-router <address1> [<address2>...<address8>]</code>
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	<code>no default-router</code>
Mode	DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. address1, address2... address8 are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	None
Format	<code>dns-server <address1> [<address2>...<address8>]</code>
Mode	DHCP Pool Config Mode

no dns-server

This command removes the DNS Server list.

Format	<code>no dns-server</code>
Mode	DHCP Pool Config Mode

hardware-address

This command specifies the hardware address of a DHCP client.

Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format.

Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	Ethernet
Format	<code>hardware-address <hardwareaddress> [type]</code>
Mode	DHCP Pool Config Mode

no hardware-address

This command removes the hardware address of the DHCP client.

Format	<code>no hardware-address</code>
Mode	DHCP Pool Config Mode

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The prefix-length is an integer from 0 to 32

Default	None
Format	<code>host <address> [mask prefix-length]</code>
Mode	DHCP Pool Config Mode

no host

This command removes the IP address of the DHCP client.

Format	<code>no host</code>
Mode	DHCP Pool Config Mode

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients.

Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	None
Format	<code>ip dhcp excluded-address <lowaddress> [highaddress]</code>
Mode	Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client.

Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format	<code>no ip dhcp excluded-address <lowaddress> [highaddress]</code>
Mode	Global Config

ip dhcp ping packets

This command is used to specify the number in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. Setting the number of ping packets to 0 is the same as 'no ip dhcp ping packets' and will prevent the server from pinging pool addresses.

Default	2
Format	<code>ip dhcp ping packets <0,2-10></code>
Mode	Global Config

no ip dhcp ping packets

This command prevents the server from pinging pool addresses and will set the number of packets to 0.

Default	0
Format	<code>no ip dhcp ping packets</code>
Mode	Global Config

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default	None
Format	<code>ip dhcp pool <name></code>
Mode	Global Config Mode

no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format	<code>no ip dhcp pool <name></code>
Mode	Global Config Mode

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If infinite is specified, lease is set for 60 days. Days is an integer from 0 to 59. Hours is an integer from 0 to 1339. Minutes is an integer from 0 to 86399.

Default	1 (day)
Format	<code>lease [<days> [hours] [minutes]] [infinite]</code>
Mode	DHCP Pool Config

no lease

This command restores the default value of the lease time for DHCP Server.

Format	<code>no lease</code>
Mode	DHCP Pool Config

network

This command is used to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	None
Format	<code>network <networknumber> [mask prefixlength]</code>
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	<code>no network</code>
Mode	DHCP Pool Config

service dhcp

This command enables the DHCP server and relay agent features on the router.

Default	Disabled
Format	<code>service dhcp</code>
Mode	Global Config

no service dhcp

This command disables the DHCP server and relay agent features.

Format	<code>no service dhcp</code>
Mode	Global Config

DHCP Server Show Commands

These commands display the DHCP Server address bindings, and statistics.

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	<code>show ip dhcp binding [address]</code>
Mode	Privileged EXEC and User EXEC
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP Address assigned to the client.
Type	The manner in which IP Address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	<code>show ip dhcp global configuration</code>
Mode	Privileged EXEC and User EXEC
Service DHCP	The field to display the status of dhcp protocol.
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Excluded Address	The ranges of IP addresses that a DHCP server should not assign to DHCP clients.

show ip dhcp pool configuration

This command displays pool configuration. If '*' is specified, configuration for all the pools is displayed.

Format	<code>show ip dhcp pool configuration {<name> *}</code>
Mode	Privileged EXEC and User EXEC
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP Address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client
Default Routers	The list of the default routers available to the DHCP client

Following additional field is displayed for Dynamic pool type

Network The network number and the mask for the DHCP address pool.

Following additional fields are displayed for Manual pool type

Client Name The name of a DHCP client.

Client Identifier The unique identifier of a DHCP client.

Hardware Address The hardware address of a DHCP client.

Hardware Address Type The protocol of the hardware platform.

Host The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Mode Privileged EXEC and User EXEC

Address Pool The number of configured address pools in the DHCP server.

Automatic bindings The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.

Manual bindings The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.

Expired bindings The number of expired leases.

Malformed messages The number of truncated or corrupted messages that were received by the DHCP server.

Message Received

DHCPREQUEST The number of DHCPREQUEST messages that were received by the server.

DHCPDECLINE The number of DHCPDECLINE messages that were received by the server.

DHCPRELEASE The number of DHCPRELEASE messages that were received by the server.

DHCPINFORM The number of DHCPINFORM messages that were received by the server.

Message Sent

DHCPOFFER	The number of DHCPOFFER messages that were sent by the server.
DHCPACK	The number of DHCPACK messages that were sent by the server.
DHCPNACK	The number of DHCPNACK messages that were sent by the server.

DHCP Server Clear Commands

These commands clear the DHCP Server address bindings, and statistics.

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If "*" is specified, the bindings corresponding to all the addresses are deleted. <address> is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	None
Format	<code>clear ip dhcp binding <address *></code>
Mode	Privileged EXEC

clear ip dhcp server statistics

This command clear DHCP server statistics counters.

Format	<code>clear ip dhcp server statistics</code>
Mode	Privileged EXEC

Appendix A IS CLI Mapping

This chapter illustrates the mapping between CLI commands and the previous 7200 Series L2 Switch commands. The Package column indicates the 7200 Series L2 Switch package in which the command is located.

Table 9-1. IS CLI Mapping

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	show serviceport	Privileged EXEC	show serviceport
Switching	show snmpcommunity	Privileged EXEC	show snmpcommunity
Switching	show snmptrap	Privileged EXEC	show snmptrap
Switching	show trapflags	Privileged EXEC	show trapflags
Switching	show telnet	Privileged EXEC and User EXEC	show remotecon
Switching	show forwardingdb agetime [fdbid all]	Privileged EXEC	show forwardingdb agetime {<fdbid> all}
Switching	config network parms <ipaddr> <netmask> [gateway]	Privileged EXEC	network parms <ipaddr> <netmask> [<gateway>]
Switching	config network protocol <none bootp dhcp>	Privileged EXEC	network protocol {none bootp dhcp}
Switching	config network webmode <enable disable>	Privileged EXEC	ip http server

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Privileged EXEC	no ip http server
Switching	config network javamode <enable disable>	Privileged EXEC	network javamode
		Privileged EXEC	no network javamode
Switching	config prompt <system prompt>	Privileged EXEC	set prompt <promptstring>
Switching	config serial baudrate <speed>	Line Config	serial baudrate {1200 2400 4800 9600 19200 38400 57600 115200}
Switching	config serial timeout <0 - 160>	Line Config	serial timeout <0-160>
Switching	config snmpcommunity accessmode <ro rw> <name>	Global Config	snmp-server community ro <name>
		Global Config	snmp-server community rw <name>
Switching	config snmpcommunity create <name>	Global Config	snmp-server community <name>
Switching	config snmpcommunity delete <name>	Global Config	no snmp-server community <name>
Switching	config snmpcommunity ipaddr <ipaddr> <name>	Global Config	snmp-server community ipaddr <ipaddr> <name>
		Global Config	no snmp-server community ipaddr <name>
Switching	config snmpcommunity ipmask <ipmask> <name>	Global Config	snmp-server community ipmask <ipmask> <name>
		Global Config	no snmp-server community ipmask <name>
Switching	config snmpcommunity mode <enable disable> <name>	Global Config	snmp-server community mode <name>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	no snmp-server community mode <name>
Switching	config snmptrap create <name> <ipaddr>	Global Config	snmptrap <name> <ipaddr>
Switching	config snmptrap delete <name> <ipaddr>	Global Config	no snmptrap <name> <ipaddr>
Switching	config snmptrap ipaddr <ipaddrold> <name> <ipaddrnew>	Global Config	snmptrap ipaddr <name> <ipaddrold> <ipaddrnew>
Switching	config snmptrap mode <enable disable> <name> <ipaddr>	Global Config	snmptrap mode <name> <ipaddr>
		Global Config	no snmptrap mode <name> <ipaddr>
Switching	config trapflags authentication <enable disable>	Global Config	snmp-server enable traps
		Global Config	no snmp-server enable traps
Switching	config trapflags bcstorm <enable disable>	Global Config	snmp-server enable traps bcstorm
		Global Config	no snmp-server enable traps bcstorm
Switching	config trapflags linkmode <enable disable>	Global Config	snmp-server enable traps linkmode
		Global Config	no snmp-server enable traps linkmode
Switching	config trapflags multiusers <enable disable>	Global Config	snmp-server enable traps multiusers
		Global Config	no snmp-server enable traps multiusers
Switching	config trapflags stpmode <enable disable>	Global Config	snmp-server enable traps stpmode

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	no snmp-server enable traps stpmode
Switching	config telnet maxsessions <0-5>	Privileged EXEC	remotecon maxsessions <0-5>
		Privileged EXEC	no remotecon maxsessions
Switching	config telnet mode <enable disable>	Privileged EXEC	telnet
		Privileged EXEC	no telnet
Switching	config telnet timeout <0-160>	Privileged EXEC	remnotecon timeout <0-160>
		Privileged EXEC	no remotecon timeout
Switching	config forwardingdb agetime <10-1,000,000> [fdbid/all]	Global Config	bridge aging-time <10-1000000> {<1-4094> all}
		Global Config	no bridge aging-time {<1-4094> all}
Switching	show spanningtree summary	Privileged EXEC and User EXEC	show spanning-tree summary
Switching	show spanningtree port <slot/port>	Privileged EXEC and User EXEC	show spanning-tree interface <slot/port>
Switching	show spanningtree cst detailed	Privileged EXEC and User EXEC	show spanning-tree

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	show spanningtree bridge	Privileged EXEC and User EXEC	show spanning-tree brief
Switching	show spanningtree mst summary	Privileged EXEC and User EXEC	show spanning-tree mst summary
Switching	show spanningtree mst detailed <mstid>	Privileged EXEC and User EXEC	show spanning-tree mst detailed <1-4094>
Switching	show spanningtree cst port summary <mstid> <slot/port/all>	Privileged EXEC and User EXEC	show spanning-tree mst port summary 0 {<slot/port> all}
Switching	show spanningtree cst port detailed <mstid> <slot/port>	Privileged EXEC and User EXEC	show spanning-tree mst port detailed 0 <slot/port>
Switching	show spanningtree vlan <vlan>	Privileged EXEC and User EXEC	show spanning-tree vlan <1-4094>
Switching	config spanningtree adminmode <enable/disable>	Global Config	spanning-tree
		Global Config	no spanning-tree
Switching	config spanningtree forceversion <802.lw/802.lw/802.ls>	Global Config	spanning-tree forceversion {802.1d 802.lw 802.ls}
		Global Config	no spanning-tree forceversion
Switching	config spanningtree configuration name <name>	Global Config	spanning-tree configuration name <name>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	no spanning-tree configuration name
Switching	config spanningtree configuration revision <0-65535>	Global Config	spanning-tree configuration revision <0-65535>
		Global Config	no spanning-tree configuration revision
Switching	config spanningtree port mode <slot/port/all> <enable/disable>	Interface Config	spanning-tree port mode all
		Interface Config	no spanning-tree port mode
Switching	config spanningtree port mode <slot/port/all> <enable/disable>	Global Config	spanning-tree port mode all
		Global Config	no spanning-tree port mode all
Switching	config spanningtree port migrationcheck <slot/port/all> <enable/disable>	Global Config	spanning-tree bpdumigrationcheck {<slot/port> all}
		Global Config	no spanning-tree bpdumigrationcheck {<slot/port> all}
Switching	config spanningtree bridge maxage <6-40>	Global Config	spanning-tree max-age <6-40>
		Global Config	no spanning-tree max-age
Switching	config spanningtree bridge hellotime <1-10>	Global Config	spanning-tree hello-time <1-10>
		Global Config	no spanning-tree hello-time
Switching	config spanningtree bridge forwarddelay <4-30>	Global Config	spanning-tree forward-time <4-30>
		Global Config	no spanning-tree forward-time

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config spanningtree bridge priority <0-61440>		Removed
Switching	config spanningtree cst port pathcost <slot/port> <1-200000000/auto>	Interface Config	spanning-tree mst 0 cost {<1-200000000> auto}
		Interface Config	no spanning-tree mst 0 cost
Switching	config spanningtree cst port priority <slot/port> <0-240>	Interface Config	spanning-tree mst 0 port-priority <0-240>
		Interface Config	no spanning-tree mst 0 port-priority
Switching	config spanningtree cst port edgeport <slot/port> <true/false>	Interface Config	spanning-tree edgeport
		Interface Config	no spanning-tree edgeport
Switching	config spanningtree mst create <mstid>	Global Config	spanning-tree mst instance <mstid>
Switching	config spanningtree mst delete <mstid>	Global Config	no spanning-tree mst instance <mstid>
Switching	config spanningtree mst vlan add <mstid> <vlan>	Global Config	spanning-tree mst vlan <mstid> <vlanid>
Switching	config spanningtree mst vlan remove <mstid> <vlan>	Global Config	no spanning-tree mst vlan <mstid> <vlanid>
Switching	config spanningtree mst priority <mstid> <0-61440>	Global Config	spanning-tree mst priority <mstid> <0-61440>
		Global Config	no spanning-tree mst priority <mstid>
Switching	config spanningtree mst port pathcost <mstid> <slot/port> <1-200000000/auto>	Interface Config	spanning-tree mst <mstid> cost {<1-200000000> auto}

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Interface Config	no spanning-tree mst <mstid> cost
Switching	config spanningtree mst port priority <mstid> <slot/port> <0-240>	Interface Config	spanning-tree mst <mstid> port-priority <0-240>
		Interface Config	no spanning-tree mst <mstid> port-priority
Switching	show inventory	Privileged EXEC	show hardware
Switching	show sysinfo	Privileged EXEC	show sysinfo
Switching	show arp switch	Privileged EXEC	show arp switch
Switching	show forwardingdb table [macaddr/all]	Privileged EXEC	show mac-addr-table [{<macaddr> all}]
Switching	show stats port detailed <slot/port>	Privileged EXEC	show interface ethernet {<slot/port> switchport}
Switching	show stats switch detailed	Privileged EXEC	
Switching	show stats port summary <slot/port>	Privileged EXEC	show interface {<slot/port> switchport}
Switching	show stats switch summary	Privileged EXEC	
Switching	show eventlog	Privileged EXEC	show eventlog
Switching	show msglog	Privileged EXEC	show msglog
Switching	show traplog	Privileged EXEC	show logging
Switching	config sysname <name>	Global Config	snmp-server sysname <name>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config syslocation <location>	Global Config	snmp-server location <loc>
Switching	config syscontact <contact>	Global Config	snmp-server contact <con>
Switching	ping <ipaddr>	Privileged EXEC and User EXEC	ping <ipaddress>
Switching	reset system	Privileged EXEC	reload
Switching	transfer upload mode <xmodem tftp>	Privileged EXEC	copy { { nvram:errorlog nvram:msglog nvram:startup-config nvram:traplog } <url> } {<url> nvram:startup-config system:image nvram:sshkey-rsa1 nvram:sshkey-rsa2 nvram:sshkey-dsa nvram:sslpem-root nvram:sslpem-server nvram:sslpem-dhweak nvram:sslpem-strong } {system:running-config nvram:startup-config}
Switching	transfer upload serverip <ipaddr>		
Switching	transfer upload path <path>		
Switching	transfer upload filename <name>		
Switching	transfer upload datatype <config errorlog msglog traplog>		
Switching	transfer upload start		
Switching	transfer download mode <xmodem tftp>		
Switching	transfer download serverip <ipaddr>		

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	transfer download path <path>		
Switching	transfer download filename <name>		
Switching	transfer download datatype <code config>		
Switching	transfer download start		
Switching	clear transfer		
Switching	save config	Privileged EXEC	copy system:running-config nvram:startup-config
Switching	clear config	Privileged EXEC	clear config
Switching	clear pass	Privileged EXEC	clear pass
Switching	clear traplog	Privileged EXEC	clear traplog
Switching	clear vlan	Privileged EXEC	clear vlan
Switching	clear lag	Privileged EXEC	clear port-channel
Switching	clear stats port <slot/port>	Privileged EXEC	clear counters [<slot/port>]
Switching	clear stats switch	Privileged EXEC	
Switching	clear igmpsnooping	Privileged EXEC	clear igmpsnooping
Switching	logout	Privileged EXEC	logout
Switching	show users info	Privileged EXEC	show users

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	show loginsession	Privileged EXEC	show loginsession
Switching	config users add <name>	Global Config	users name <username>
Switching	config users delete <name>	Global Config	no users name <username>
Switching	config users passwd <user>	Global Config	users passwd <username>
Switching	config users snmpv3 authentication <user> <none/md5/sha>	Global Config	users snmpv3 authentication <username> {none md5 sha}
		Global Config	no users snmpv3 authentication <username>
Switching	config users snmpv3 encryption <user> <none/des [key]>	Global Config	users snmpv3 encryption <username> {none des [key]}
		Global Config	no users snmpv3 encryption <username>
Switching	config users snmpv3 accessmode <user> <readonly/readwrite>	Global Config	users snmpv3 accessmode <username> {readonly readwrite}
		Global Config	no users snmpv3 accessmode <username>
Switching	config loginsession close <sessionID/all>	Privileged EXEC	disconnect {<sessionID> all}
Switching	show switchconfig	Privileged EXEC	show storm-control
Switching	show port <slot/port all>	Privileged EXEC	show port {<slot/port> all}
Switching	show lag <logical slot/port all>	Privileged EXEC	show port-channel {<logical slot/port> all}

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	show lags summary	Privileged EXEC and User EXEC	show port-channel brief
Switching	show vlan summary	Privileged EXEC and User EXEC	show vlan brief
Switching	show vlan detailed <vlan-id>	Privileged EXEC and User EXEC	show vlan <vlanid>
Switching	show vlan port <slot/port>	Privileged EXEC and User EXEC	show vlan port {<slot/port> all}
Switching	show protocol <groupid/all>	Privileged EXEC	show port protocol {<groupid> all}
Switching	show garp info	Privileged EXEC and User EXEC	show garp
Switching	show garp interface <slot/port/all>	Privileged EXEC and User EXEC	show gmrp configuration {<slot/port> all}
		Privileged EXEC and User EXEC	show gvrp configuration {<slot/port> all}
Switching	show igmpsnooping	Privileged EXEC	show igmpsnooping
Switching	show mfdb table [macaddr/all]	Privileged EXEC	show mac-address-table multicast [{<macaddr> all}]

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	show mfdb gmrp	Privileged EXEC	show mac-address-table gmrp
Switching	show mfdb igmpsnooping	Privileged EXEC	show mac-address-table igmpsnooping
Switching	show mfdb statisticfiltering	Privileged EXEC	show mac-address-table staticfiltering
Switching	show mfdb stats	Privileged EXEC	show mac-address-table stats
Switching	show mirroring	Privileged EXEC	show monitor
Switching	config switchconfig broadcast <enable/disable>	Global Config	storm-control broadcast
		Global Config	no storm-control broadcast
Switching	config switchconfig flowcontrol <enable/disable>	Global Config	storm-control flowcontrol
		Global Config	no storm-control flowcontrol
Switching	config port adminmode <slot/port all> <enable disable>	Interface Config	shutdown
		Interface Config	no shutdown
		Global Config	shutdown all
		Global Config	no shutdown all
Switching	config port linktrap <slot/port all> <enable disable>	Interface Config	snmp trap link- status
		Interface Config	no snmp trap link- status

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	snmp trap link- status all
		Global Config	no snmp trap link- status all
Switching	config port physicalmode <slot/port all> <100h 100f 10h 10f>	Interface Config	speed {{100 10} {half-duplex full-duplex} 1000 full-duplex}
		Global Config	speed all {{100 10} {half-duplex full-duplex} 1000 full-duplex}
Switching	config port lacpmode <slot/port/all> <enable/disable>	Interface Config	port lacpmode
		Interface Config	no port lacpmode
		Global Config	port lacpmode all
		Global Config	no port lacpmode all
Switching	config port autoneg <slot/port/all> <enable/disable>	Interface Config	auto-negotiate
		Interface Config	no auto-negotiate
		Global Config	auto-negotiate all
		Global Config	no auto-negotiate all
Switching	config lag create <name>	Global Config	port-channel <name>
Switching	config lag addport <logical slot/port> <slot/port>	Interface Config	addport <logical slot/port>
Switching	config lag deleteport <logical slot/port> <slot/port all>	Interface Config	deleteport <logical slot/port>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	deleteport <logical slot/port> all
Switching	config lag adminmode <logical slot/port all> <enable disable>	Global Config	port-channel adminmode {<logical slot/port> all}
		Global Config	no port-channel adminmode {<logical slot/port> all}
Switching	config lag linktrap <logical slot/port all> <enable disable>	Global Config	port-channel linktrap {<logical slot/port> all}
		Global Config	no port-channel linktrap {<logical slot/port> all}
Switching	config lag name <logical slot/port all> <name>	Global Config	port-channel name {<logical slot/port> all} <name>
Switching	config lag deletelag <logical slot/port all>	Interface Config	delete interface {<logical slot/port> all}
Switching	config lag stpmode <logical slot/port all> <off 802.1d fast>	Interface Config	spanning-tree {<logical slot/port> all} {off 802.1d fast}
Switching	config vlan create <2-4094>	VLAN database	vlan <1-4094>
		VLAN database	no vlan <1-4094>
Switching	config vlan name <name> <2-4094>	VLAN database	vlan name <1-4094> <newname>
Switching	config vlan delete <2-4094>	VLAN database	no vlan name <1-4094>
Switching	config vlan makestatic <2-4094>	VLAN database	vlan makestatic <1-4094>
Switching	config vlan participation <exclude include auto> <1-4094> <slot/port all>	Interface Config	vlan participation {exclude include auto} <1-4094>
		Global Config	vlan participation all {exclude include auto} <1-4094>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config vlan port tagging <enable disable> <1-4094> <slot/port all>	Interface Config	vlan tagging <1-4094>
		Interface Config	no vlan tagging <1-4094>
		Global Config	vlan port tagging all <1-4094>
		Global Config	no vlan port tagging all <1-4094>
Switching	config vlan port pvid <1-4094> <slot/port all>	Interface Config	vlan pvid <1-4094>
		Global Config	vlan port pvid all <1-4094>
Switching	config vlan port acceptframe <all vlan> <slot/port all>	Interface Config	vlan acceptframe {vlanonly all}
		Interface Config	no vlan acceptframe
		Global Config	vlan port acceptframe all {vlanonly all}
		Global Config	no vlan port acceptframe all
Switching	config vlan port ingressfilter <enable disable> <slot/port all>	Interface Config	vlan ingressfilter
		Interface Config	no vlan ingressfilter
		Global Config	vlan port ingressfilter all
		Global Config	no vlan port ingressfilter all
Switching	config protocol create <groupname>	Global Config	vlan protocol group <groupname>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config protocol delete <groupid>	Global Config	vlan protocol group remove <groupid>
Switching	config protocol protocol add <groupid> <protocol>	Global Config	vlan protocol group add protocol <groupid> {ip arp ipx}
Switching	config protocol protocol remove <groupid> <protocol>	Global Config	no vlan protocol group add protocol <groupid> {ip arp ipx}
Switching	config protocol vlan add <groupid> <vlan>	VLAN database	protocol group <groupid> <1-4094>
Switching	config protocol vlan remove <groupid> <vlan>	VLAN database	no protocol group <groupid> <1-4094>
Switching	config protocol interface add <groupid> <slot/port / all>	Interface Config	protocol vlan group <groupid>
Switching	config protocol interface remove <groupid> <slot/port/all>	Interface Config	no protocol vlan group <groupid>
Switching	config protocol interface remove <groupid> <slot/port/all>	Global Config	protocol vlan group all <groupid>
Switching	config protocol interface remove <groupid> <slot/port/all>	Global Config	no protocol vlan group all <groupid>
Switching	config garp gmrp adminmode <enable/disable>	Privileged EXEC	set gmrp adminmode
		Privileged EXEC	no set gmrp adminmode
Switching	config garp gmrp interfacemode <slot/port/all> <enable/disable>	Interface Config	set gmrp interfacemode
		Interface Config	no set gmrp interfacemode
		Global Config	set gmrp interfacemode all
		Global Config	no set gmrp interfacemode all

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config garp gvrp adminmode <enable disable>	Privileged EXEC	set gvrp adminmode
		Privileged EXEC	no set gvrp adminmode
Switching	config garp gvrp interfacemode <slot/port all> <enable disable>	Interface Config	set gvrp interfacemode
		Interface Config	no set gvrp interfacemode
		Global Config	set gvrp interfacemode all
		Global Config	no set gvrp interfacemode all
Switching	config garp jointimer <slot/port/all> <10-100>	Interface Config	set garp timer join <10-100>
		Interface Config	no set garp timer join
		Global Config	set garp timer join all <10-100>
		Global Config	no set garp timer join all
Switching	config garp leavetimer <slot/port/ all> <20-600>	Interface Config	set garp timer leave <20-600>
		Interface Config	no set garp timer leave
		Global Config	set garp timer leave all <20-600>
		Global Config	no set garp timer leave all
Switching	config garp leavealltimer <slot/port/ all> <200-600>	Interface Config	set garp timer leaveall <200-6000>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Interface Config	no set garp timer leaveall
		Global Config	set garp timer leaveall all <200-6000>
		Global Config	no set garp timer leaveall all
Switching	config igmpsnooping adminmode <enable/disable>	Global Config	set igmp
		Global Config	no set igmp
Switching	config igmpsnooping groupmembershipinterval <1-3600>	Global Config	set igmp groupmembershipinterval <2-3600>
		Global Config	no set igmp groupmembershipinterval
Switching	config igmpsnooping maxresponse <1-3600>	Global Config	set igmp maxresponse <1-3599>
		Global Config	no set igmp maxresponse
Switching	config igmpsnooping mcrtexpiretime <0-3600>	Global Config	set igmp mcrtexpiretime <0-3600>
		Global Config	no set igmp mcrtexpiretime
Switching	config igmpsnooping interfacemode <slot/port/all> <enable/disable>	Interface Config	set igmp
		Interface Config	no set igmp
		Global Config	set igmp interfacemode all

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Switching	config mirroring delete	Global Config	no set igmp interfacemode all
Switching	config mirroring create <slot/port> <slot/port>	Global Config	monitor session source <slot/port> destination <slot/port>
		Global Config	no monitor session
Switching	config mirroring mode <enable disable>	Global Config	monitor session mode
		Global Config	no monitor session mode
Security	config authentication login create <listname>	Global Config	authentication login <listname> [method1 [method2 [method3]]]
Security	config authentication login set <listname> <local/radius/reject> [local/radius/reject] [local/radius/reject]	Global Config	
Security	config authentication login delete <listname>	Global Config	no authentication login <listname>
Security	config users defaultlogin <listname>	Global Config	users defaultlogin <listname>
Security	config users login <user> <listname>	Global Config	users login <user> <listname>
Security	show authentication login info	Privileged EXEC	show authentication
Security	show authentication login users <listname>	Privileged EXEC	show authentication users <listname>
Security	show users authentication	Privileged EXEC	show users authentication
Security	config radius maxretransmit <1 - 15>	Global Config	radius server retransmit <1-15>

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Global Config	no radius server retransmit
Security	config radius timeout <1 - 30>	Global Config	radius server timeout <1-30>
		Global Config	no radius server timeout
Security	config radius accounting mode <enable/disable>	Global Config	radius accounting mode
		Global Config	no radius accounting mode
Security	config radius accounting server add <ipaddr>	Global Config	radius server host {auth acct} <ipaddr> [<0-65535>]
Security	config radius accounting server port <ipaddr> <0 - 65535>	Global Config	
Security	config radius accounting server remove <ipaddr>	Global Config	
Security	config radius server add <ipaddr>	Global Config	
Security	config radius server port <ipaddr> <0 - 65535>	Global Config	
Security	config radius server remove <ipaddr>	Global Config	no radius server host {auth acct} <ipaddr>
Security	config radius accounting server secret <ipaddr>	Global Config	radius server key {auth acct} <ipaddr>
Security	config radius server secret <ipaddr>	Global Config	
Security	config radius server primary <ipaddr>	Global Config	radius server primary <ipaddr>
Security	show radius summary	Privileged EXEC	show radius [servers]

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Security	show radius server summary	Privileged EXEC	
Security	show radius server stats <ipaddr>	Privileged EXEC	show radius statistics <ipaddr>
Security	show radius accounting summary	Privileged EXEC	show radius accounting [statistics <ipaddr>]
Security	show radius accounting stats <ipaddr>	Privileged EXEC	
Security	show radius stats	Privileged EXEC	show radius statistics
Security	clear radius stats	Privileged EXEC	clear radius statistics
Security	config dot1x adminmode <enable/disable>	Global Config	dot1x system-auth-control
		Global Config	no dot1x system-auth-control
Security	config dot1x port initialize <slot/port>	Privileged EXEC	dot1x initialize <slot/port>
Security	config dot1x port reauthenticate <slot/port>	Privileged EXEC	dot1x re-authenticate <slot/port>
Security	config dot1x port controldir <slot/port/all> <both/in>		Removed
Security	config dot1x port controlmode <slot/port/all> <forceunauthorized/forceauthorized/auto>	Global Config	dot1x port-control all {force-unauthorized force-authorized auto}
		Global Config	no dot1x port-control all
		Interface Config	dot1x port-control {force-unauthorized force-authorized auto}

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
		Interface Config	no dot1x port-control
Security	config dot1x port quietperiod <slot/port> <0-65535>	Interface Config	dot1x timeout {{reauth-period <seconds>} {quiet-period <seconds>} {tx-period <seconds>} {supp-timeout <seconds>} {server-timeout <0-65535>}}
Security	config dot1x port transmitperiod <slot/port> <1-65535>	Interface Config	no dot1x timeout {reauth-period quiet-period tx-period supp-timeout server-timeout}
Security	config dot1x port supptimeout <slot/port> <1-65535>	Interface Config	
Security	config dot1x port servertimeout <slot/port> <1-65535>	Interface Config	
Security	config dot1x port reauthperiod <slot/port> <1-65535>	Interface Config	
Security	config dot1x port maxrequests <slot/port> <1-10>	Interface Config	dot1x max-req <1-10>
		Interface Config	no dot1x max-req
Security	config dot1x port reauthenabled <slot/port> <true/false>	Interface Config	dot1x re-authentication
		Interface Config	no dot1x re-authentication
Security	config dot1x defaultlogin <listname>	Global Config	dot1x defaultlogin <listname>
Security	config dot1x login <user> <listname>	Global Config	dot1x login <user> <listname>
Security	config dot1x port users add <user> <slot/port/all>	Global Config	dot1x user <user> {<slot/port> all}
Security	config dot1x port users remove <user> <slot/port/all>	Global Config	no dot1x user <user> {<slot/port> all}

Table 9-1. IS CLI Mapping (continued)

Package	7200 Series L2 Switch Command	CLI Command	
		Mode	Syntax
Security	show dot1x summary	Privileged EXEC	show dot1x [{summary {<slot/port> all}} {detail <slot/port>} {statistics <slot/port>} {users <slot/port>}]
Security	show dot1x port summary <slot/port/all>	Privileged EXEC	
Security	show dot1x port detailed <slot/port>	Privileged EXEC	
Security	show dot1x port stats <slot/port>	Privileged EXEC	
Security	show dot1x port users <slot/port>	Privileged EXEC	
Security	clear dot1x port stats <slot/port/all>	Privileged EXEC	clear dot1x statistics {<slot/port> all}

Appendix B

Cabling Guidelines

This appendix provides specifications for cables used with a NETGEAR NETGEAR 7200 Series 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.

The Table below lists the electrical requirements of Category 5 UTP cable.

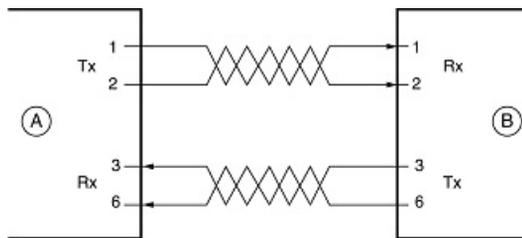
Table 9-2. Electrical Requirements of Category 5 Cable

SPECIFICATIONS	CATEGORY 5 CABLE REQUIREMENTS
Number of pairs	Four
Impedance	100 ± 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.

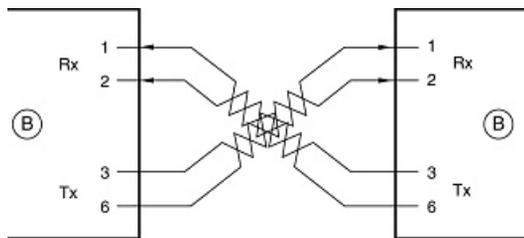
Figure 9-1 illustrates straight-through twisted pair cable.



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 9-1: Straight-Through Twisted-Pair Cable

Figure 9-2 illustrates crossover twisted pair cable.



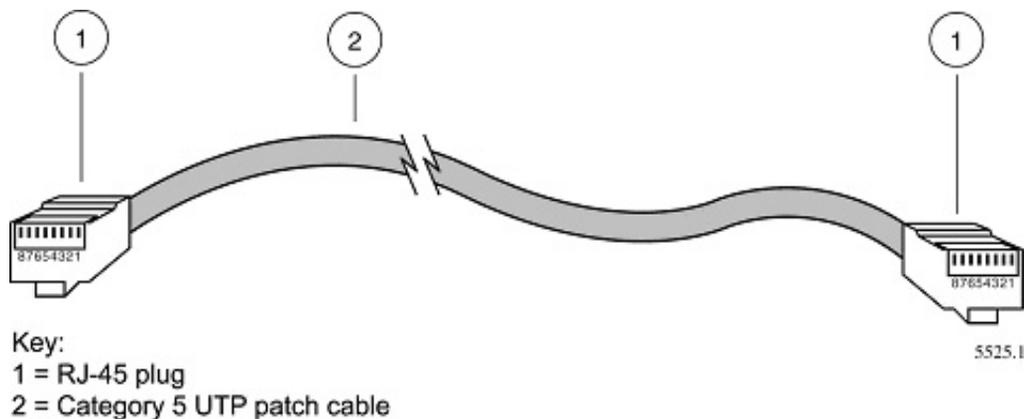
Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure 9-2: 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 9-3: 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.

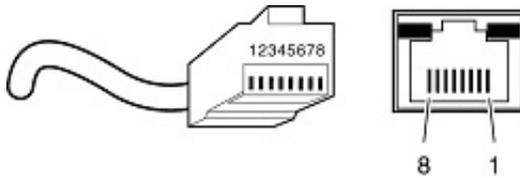
Patch Cables

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 9-4 shows the RJ-45 plug and RJ-45 connector.



Key:
1 to 8 = pin numbers

Figure 9-4: RJ-45 Plug and RJ-45 Connector with Built-in LEDs

Table 9-1 lists the pin assignments for the 10/100 Mbps RJ-45 plug and the RJ-45 connector.

Table 9-1. 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 9-2. 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 C

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 18 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

Address Resolution Protocol

An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

Advanced Network Device Layer/Software

Term for the Device Driver level.

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.

Area Border Router

A router located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are considered members of both the OSPF backbone and the attached areas. They therefore maintain routing tables describing both the backbone topology and the topology of the other areas. (Cisco Systems Inc.)

ARP

See “Address Resolution Protocol” on page 2.

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.

Backbone

The part of a network used as a primary path for transporting traffic between network segments.

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

BPDU is 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.

Capacity planning

Determining whether current solutions can satisfy future demands. Capacity planning includes evaluating potential workload and infrastructure changes.

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.

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

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.

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 5.

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.

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.

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 17 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.

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 a 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 8.

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.

hop count

The number of routers that a data packet passes through on its way to its destination.

I

ICMP

See “Internet Control Message Protocol” on page 9.

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 9.

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 9 for more information.

Internet Control Message Protocol

ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

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.

Link-State

In routing protocols, the declared information about the available interfaces and available neighbors of a router or network. The protocol's topological database is formed from the collected link-state declarations.

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.

MBONE

See "Multicast Backbone" on page 12.

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 11.

Multicast Backbone

The MBONE is a virtual network. It is layered on top of portions of the physical Internet to support routing of IP multicast packets since that function has not yet been integrated into many production routers. The network is composed of islands that can directly support IP multicast, such as multicast LANs like Ethernet, linked by virtual point-to-point links called "tunnels". The tunnel endpoints are typically workstation-class machines having operating system support for IP multicast and running the "mrouted" multicast routing daemon.

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 12.

N

NAT

See "Network Address Translation" on page 12.

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.

Network Address Translation

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

nm

Nanometer (1 x 10^{e9}) 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 13.

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 14.

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.

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 14.

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.

Real-Time Operating System

RTOS is a component of the OSAPI module that abstracts operating systems with which other systems can interface.

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.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

RIPng

Routing Information Protocol, new generation.

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 15.

RTOS

See “Real-Time Operating System” on page 15.

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 16.

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 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 16.

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 “TLS” on page 17.

TLS

Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the

TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

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 combing 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

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 18.

W

WAN

See “Wide Area Network” on page 19.

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.

