



24-Port 10/100/1000Mbps Ethernet Security Switch

WGSW-24000

User's Manual

Trademarks

Copyright © PLANET Technology Corp. 2005.

Contents subject to which revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

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

CE Mark Warning

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

Revision

PLANET Fast Ethernet Switch User's Manual

FOR MODELS: WGSW-24000

Part No. 2081-A93050-000

Table of Contents

1. INTRODUCTION	12
1.1 Packet Contents.....	12
1.2 How to Use This Manual.....	12
1.3 Product Feature	12
1.4 Product Specification	13
2. INSTALLATION.....	15
2.1 Product Description.....	15
2.1.1 Product Overview	15
2.1.2 Switch Front Panel	15
2.1.3 LED Indications	16
2.1.4 Switch Rear Panel.....	16
2.2 Install the Switch	16
2.2.1 Desktop Installation.....	16
2.2.2 Rack Mounting	17
3. CONFIGURATION.....	19
3.1 Management Access Overview	19
3.1.1 Administration Console	20
3.1.2 Direct Access.....	20
3.2 Web Management.....	20
3.3 SNMP-Based Network Management.....	21
3.4 Protocols	21
3.4.1 Virtual Terminal Protocols.....	21
3.4.2 SNMP Protocol.....	21
3.4.3 Management Architecture	21
4. COMMAND STRUCTURE	23
4.1 Format.....	23
4.1.1 Command.....	23
4.1.2 Parameters.....	23
4.1.3 Values.....	24
4.1.4 Conventions	24
4.1.5 Annotations.....	24
5. QUICK START UP	26
5.1 Quick Starting the Switch	26
5.2 System Info and System Setup	26
6. MODE-BASED CLI	31
6.1 Mode-Based Topology	32

6.2 Mode-based Command Hierarchy	33
6.3 Flow of Operation.....	35
6.4 "No" Form of a Command.....	36
6.4.1 Support for "No" Form.....	36
6.4.2 Behavior of Command Help ("?").....	36
7. CLI Commands: Base	38
7.1 System Information and Statistics Commands	38
7.1.1 show arp switch.....	38
7.1.2 show eventlog	38
7.1.3 show hardware	39
7.1.4 show interface	39
7.1.5 show interface ethernet.....	40
7.1.6 show logging	46
7.1.7 show mac-addr-table.....	47
7.1.8 show msglog	47
7.1.9 show running-config	47
7.1.10 show sysinfo.....	48
7.1.11 snmp-server.....	48
7.2 Management VLAN Commands	48
7.2.1 network mgmt_vlan	48
7.3 Dot1P Commands.....	48
7.3.1 classofservice dot1pmapping.....	48
7.3.2 show classofservice dot1pmapping	49
7.3.3 vlan port priority all	49
7.3.4 vlan priority	49
7.4 LAG/Port-Channel (802.3ad) Commands	49
7.4.1 port-channel staticcapability.....	49
7.4.2 show port-channel brief.....	50
7.5 Management Commands	50
7.5.1 bridge aging-time	50
7.5.2 mtu	51
7.5.3 network javamode	51
7.5.4 network mac-address.....	51
7.5.5 network mac-type.....	52
7.5.6 network parms.....	52
7.5.7 network protocol.....	52
7.5.8 remotecon maxsessions	52
7.5.9 remotecon timeout	53

7.5.10 serial baudrate	53
7.5.11 serial timeout	53
7.5.12 set prompt	54
7.5.13 show forwardingdb agetime	54
5.7.14 show network	54
7.5.15 show remotecon	55
7.5.16 show serial	55
7.5.17 show snmpcommunity.....	56
7.5.18 show snmptrap	56
7.5.19 show trapflags	57
7.5.20 snmp-server community.....	57
7.5.21 snmp-server community ipaddr.....	58
7.5.22 snmp-server community ipmask	58
7.5.23 snmp-server community mode.....	59
7.5.24 snmp-server community ro.....	59
7.5.25 snmp-server community rw	59
7.5.26 snmp-server enable traps	59
7.5.28 snmp-server enable traps linkmode.....	60
7.5.29 snmp-server enable traps multiusers.....	60
7.5.30 snmp-server enable traps stpmode	61
7.5.31 snmptrap	61
7.5.32 snmptrap ipaddr	61
7.5.33 snmptrap mode	62
7.5.34 telnet.....	62
7.6 Device Configuration Commands	62
7.6.1 addport	62
7.6.2 auto-negotiate	63
7.6.3 auto-negotiate all.....	63
7.6.4 delete interface.....	63
7.6.5 deleteport	63
7.6.6 macfilter	63
7.6.7 macfilter adddest.....	64
7.6.8 macfilter adddest all	64
7.6.9 macfilter addsrc.....	65
7.6.10 macfilter addsrc all	65
7.6.11 monitor session	66
7.6.12 monitor session mode.....	66
7.6.13 port lacpmode	66

7.6.14 port lacpmode all	67
7.6.15 port-channel	67
7.6.16 port-channel adminmode	67
7.6.17 port-channel linktrap.....	67
7.6.18 port-channel name	68
7.6.19 protocol group	68
7.6.20 protocol vlan group.....	68
7.6.21 protocol vlan group all	69
7.6.22 set garp timer join.....	69
7.6.23 set garp timer join all	70
7.6.24 set garp timer leave.....	70
7.6.25 set garp timer leave all	70
7.6.26 set garp timer leaveall	71
7.6.27 set garp timer leaveall all	71
7.6.28 set gmrp adminmode	72
7.6.29 set gmrp interfacemode	72
7.6.30 set gmrp interfacemode all.....	73
7.6.31 set gvrp adminmode.....	73
7.6.32 set gvrp interfacemode.....	73
7.6.33 set gvrp interfacemode all	74
7.6.34 show description	74
7.6.35 show garp.....	74
7.6.36 show gmrp configuration	74
7.6.37 show gvrp configuration	75
7.6.38 show igmpsnooping	76
7.6.39 show mac-address-table gmrp.....	77
7.6.40 show mac-address-table igmpsnooping.....	77
7.6.41 show mac-address-table multicast.....	77
7.6.42 show mac-address-table static.....	78
7.6.43 show mac-address-table staticfiltering	78
7.6.44 show mac-address-table stats	78
7.6.45 show monitor	79
7.6.46 show port.....	79
7.6.47 show port protocol.....	80
7.6.48 show port-channel.....	80
7.6.49 show storm-control.....	81
7.6.50 show vlan	81
7.6.51 show vlan brief	82

7.6.52 show vlan port	82
7.6.53 shutdown	83
7.6.54 shutdown all	83
7.6.55 snmp trap link-status	83
7.6.56 snmp trap link-status all	83
7.6.57 spanning-tree	84
7.6.58 spanning-tree bpdumigrationcheck	84
7.6.59 description	84
7.6.60 speed.....	85
7.6.61 speed all	85
7.6.62 storm-control broadcast	85
7.6.63 storm-control flowcontrol	86
7.6.64 vlan	86
7.6.65 vlan acceptframe	87
7.6.66 vlan ingressfilter	87
7.6.67 vlan makestatic.....	88
7.6.68 vlan name.....	88
7.6.69 vlan participation	88
7.6.70 vlan participation all.....	88
7.6.71 vlan port acceptframe all	89
7.6.72 vlan port ingressfilter all	89
7.6.73 vlan port pvid all	90
7.6.74 vlan port tagging all	90
7.6.75 vlan protocol group.....	90
7.6.76 vlan protocol group add protocol.....	90
7.6.77 vlan protocol group remove.....	91
7.6.78 vlan pvid	91
7.6.79 vlan tagging	91
7.7 User Account Management Commands	92
7.7.1 disconnect	92
7.7.2 show login session	92
7.7.3 show users	92
7.7.4 users name.....	93
7.7.5 users passwd	93
7.7.6 users snmpv3 accessmode.....	94
7.7.7 users snmpv3 authentication	94
7.7.8 users snmpv3 encryption	94
7.8 System Utilities	95

7.8.1 clear config	95
7.8.2 clear counters.....	95
7.8.3 clear igmpsnooping	95
7.8.4 clear pass	95
7.8.5 clear port-channel	96
7.8.6 clear traplog.....	96
7.8.7 clear vlan	96
7.8.8 copy.....	96
7.8.9 logout.....	97
7.8.10 ping.....	97
7.8.11 reload.....	97
8. CLI COMMANDS: QUALITY OF SERVICE	98
8.1 CLI Commands: Access Control List	98
8.1.1 show ip access-lists	98
8.2 Configuration Commands	98
8.2.1 access-list.....	98
8.2.2 ip access-group	99
8.2.3 ip access-group all	99
8.3 CLI Commands: Differentiated Services.....	100
8.3.1 diffserv	101
8.4 Class Commands.....	101
8.4.1 class-map	102
8.4.2 class-map rename.....	103
8.4.3 match any.....	103
8.4.4 match class-map	103
8.4.5 match destination-address mac	104
8.4.6 match dstip	104
8.4.7 match dstl4port.....	104
8.4.8 match ip dscp	105
8.4.9 match ip precedence.....	105
8.4.10 match ip tos	106
8.4.11 match protocol	106
8.4.12 match source-address mac.....	107
8.4.13 match srcip	107
8.4.14 match srcl4port.....	107
8.4.15 match vlan	108
8.5 Policy Commands	108
8.5.1 bandwidth kbps	109

8.5.2 bandwidth percent.....	109
8.5.3 class	110
8.5.4 expedite kbps	110
8.5.5 expedite percent.....	111
8.5.6 mark ip-dscp.....	111
8.5.7 mark ip-precedence	111
8.5.8 police-simple	112
8.5.9 police-single-rate.....	112
8.5.10 police-two-rate.....	113
8.5.11 policy-map	113
8.5.12 policy-map rename.....	114
8.5.13 randomdrop	114
8.5.14 shape bps-average	115
8.5.15 shape bps-peak.....	115
8.6 Service Commands.....	116
8.6.1 service-policy.....	116
8.7 Show Commands.....	117
8.7.1 show class-map	117
8.7.2 show diffserv	118
8.7.3 show policy-map	118
8.7.4 show diffserv service.....	120
8.7.5 show diffserv service brief.....	121
8.7.6 show policy-map interface.....	121
8.7.7 show service-policy	122
8.8 Rate-Limiting Commands	123
8.8.1 rate-limiting.....	123
8.8.2 show rate-limiting	123
9. CLI COMMANDS: SECURITY	125
9.1 Security Commands.....	125
9.1.1 authentication login	125
9.1.2 clear dot1x statistics	126
9.1.3 clear radius statistics.....	126
9.1.4 dot1x defaultlogin	126
9.1.5 dot1x initialize.....	126
9.1.6 dot1x login	126
9.1.7 dot1x max-req	126
9.1.7.1 no dot1x max-req	127
9.1.8 dot1x port-control	127

9.1.9 dot1x port-control All	127
9.1.10 dot1x re-authenticate	128
9.1.11 dot1x re-authentication	128
9.1.12 dot1x system-auth-control	128
9.1.13 dot1x timeout	128
9.1.15 radius accounting mode	130
9.1.16 radius server host	130
9.1.17 radius server key	131
9.1.18 radius server msgauth	131
9.1.19 radius server primary	131
9.1.20 radius server retransmit	131
9.1.21 radius server timeout	132
9.1.22 show accounting	132
9.1.23 show authentication	133
9.1.24 show authentication users	133
9.1.25 show dot1x	133
9.1.26 show dot1x users	136
9.1.27 show radius	136
9.1.28 show radius statistics	136
9.1.29 show users authentication	137
9.1.30 users defaultlogin	137
9.1.31 users login	138
9.2 Secure Shell (SSH) Commands	138
9.2.1 ip ssh	138
9.2.2 ip ssh protocol	138
9.2.3 show ip ssh	139
9.3 HTTP Commands	139
9.3.1 ip http secure-port	139
9.3.2 ip http secure-protocol	139
9.3.3 ip http secure-server	139
9.3.4 ip http server	140
9.3.5 show ip http	140
9.4 MAC Lock Commands	141
9.4.1 mac-lock	141
9.4.2 show mac-lock	141
10. CLI COMMANDS: SWITCHING	142
10.1 Spanning Tree Commands	142
10.1.1 show spanning-tree	142

10.1.2 show spanning-tree interface	143
10.1.3 show spanning-tree mst detailed	143
10.1.4 show spanning-tree mst port detailed	144
10.1.5 show spanning-tree mst port summary	145
10.1.6 show spanning-tree mst summary	145
10.1.7 show spanning-tree summary	145
10.1.8 show spanning-tree vlan	146
10.1.9 spanning-tree	146
10.1.10 spanning-tree configuration name	146
10.1.11 spanning-tree configuration revision	147
10.1.12 spanning-tree edgeport	147
10.1.13 spanning-tree forceversion.....	147
10.1.14 spanning-tree forward-time	148
10.1.15 spanning-tree hello-time.....	148
10.1.16 spanning-tree max-age	148
10.1.17 spanning-tree mst	149
10.1.18 spanning-tree mst instance	150
10.1.19 spanning-tree mst priority.....	150
10.1.20 spanning-tree mst vlan.....	151
10.1.21 spanning-tree port mode	151
10.1.22 spanning-tree port mode all	151
11. USING THE WEB INTERFACE.....	152
11.1 Configuring for Web Access.....	152
11.1.1 Web Page Layout.....	152
11.1.2 Starting the Web Interface.....	153
11.1.3 Command Buttons.....	153
12. SWITCH OPERATION	154
12.1 Address Table	154
12.2 Learning	154
12.3 Forwarding & Filtering.....	154
12.4 Store-and-Forward.....	154
12.5 Auto-Negotiation	155
13. TROUBLE SHOOTING	156
APPENDEX A.....	157
A.1 Switch's RJ-45 Pin Assignments	157
A.2 10/100Mbps, 10/100Base-TX.....	157

1. INTRODUCTION

1.1 Packet Contents

Check the contents of your package for following parts:

- Gigabit Ethernet Security Switch x1
- CD-ROM user's manual x1
- Quick installation guide x1
- 19" rack mounting kit x1
- Power cord x1
- Rubber feet x 4

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

1.2 How to Use This Manual

This User Manual is structured as follows:

Section 2, **Installation**

The section explains the functions of the Switch and how to physically install the Switch.

Section 3, **Configuration**

The section contains the information about the software function of the Switch.

Section 4, **Switch Operation**

The section contains specifications of the Switch.

Appendices

The section contains cable information of the Switch.

In the following section, terms "**SWITCH**" with upper case denotes the WGSW-24000 Ethernet switch.

Terms with lower case "switch" means any Ethernet switches.

1.3 Product Feature

- 24 10/100/1000Mbps auto-negotiation ports.
- Supports half duplex and full duplex modes and auto-negotiation for all 10BaseT/100BaseTX/1000BaseT ports.
- MDI/MDI-X auto-sense on all ports and IEEE 802.3ab Auto MDI/MDI-X on all 100/1000 twisted-pair ports.
- Supports up to four Class of Server (CoS) queues per egress port.
- Implements two mechanisms, cell-based HOL blocking and packet-based HOL blocking, to

- prevent Head of Line Blocking on a per-port basis.
- Supports a packet aging mechanism, which allows the switch to discard a packet residing in the packet memory. The packet age limit is programmable and has maximum time duration of approximately 515 seconds.
- Supports mechanisms to handle backpressure allowing for flexible flow control on packet transactions. The limit at which backpressure is detected is based on the amount of memory utilized by the packets on an input port. This limit is programmable on a per-port basis.
- Provides programmable threshold limits to prevent packets from flooding into other parts of the network. Three types of packet can be monitored and separate counters are maintained for each type of packet.
- Full compliant with the IEEE 802.1D spanning tree support specifications.
- Supports the IEEE 802.1s specification for multiple spanning trees on a single port (spanning tree per VLAN).
- Supports the IEEE 802.1p specification for traffic class expediting and dynamic multicast filtering support (Class of Service, or CoS).
- Supports the IEEE 802.1Q Specification for Virtual Bridged Local Area Network.
- Provides a mechanism by which up to eight ports of the same speed can be bundled together to form a port bundle or a trunk group. Up to six trunk groups can be established.
- Supports inclusive and exclusive filtering to enable a switch application to filter and classify packets based on certain protocol fields in the packet.
- Supports mirroring to monitor the incoming or outgoing traffic on a particular port.

1.4 Product Specification

Model	WGSW-24000
Network Ports	24-port RJ-45 for 10/100TX 2 mini-GBIC
Speed	24-Port: 10/100Mbps at half duplex, 20/200Mbps at full duplex
	Mini-GBIC: 10/100/1000Mbps at half duplex, 20/200/2000Mbps at full duplex
Switch architecture	Store and forward switch architecture. Back-plan up to 48Gbps
MAC address	8K MAC address table with Auto learning function
Memory	64Mbits for packet buffer
LED	Power, Link/Act, 100 Mbps, FDX/COL Module: Link/Act, 1000 Mbps, FDX/COL
Management Interface	Console. Telnet, SSH, Web, SSL, SNMP
Operating Temperature	0°C~40°C,
Storage Temperature	-40°C~70°C,
Operating Humidity	20% to 85%, relative humidity, non-condensing

Storage Humidity	20% to 90%, relative humidity, non-condensing
Operating Temperature	0°C~40°C,
Dimension	430mm(W) x 350mm(D) x 44.5mm(H)
Weight	5.0 kg
EMI	FCC Class A, CE
Standard Compliance	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3z Gigabit SX/LX IEEE802.3ab Gigabit 1000T IEEE802.3x Flow Control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning tree protocol IEEE802.1w Rapid spanning tree protocol IEEE802.1p Class of service IEEE802.1Q VLAN Tagging

2. INSTALLATION

This section describes the functionalities of the Switch's components and guides how to install it on the desktop or shelf. Basic knowledge of networking is assumed. Please read this chapter completely before continuing.

2.1 Product Description

The PLANET WGSW-24000 is a 24-Port 10/100/1000Mbps with 2 shared SFP/copper GbE interface Gigabit Ethernet Switch. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 48Gbps. Its two built-in GbE uplink ports also offer incredible extensibility, flexibility and connectivity to the Core switch or Servers.

2.1.1 Product Overview

PLANET WGSW-24000 is loaded with powerful traffic management and QoS features to enhance services offered by telcos. It provides 4 priority queues per port for different types of traffics, allowing administrators to set policies for classified filtering and rule-based rate limitation. The WGSW-24000 prioritizes applications with WFQ (Weighted Fair Queuing) scheduling algorithm to allocate more bandwidth to key traffics such as voice transmission, empowering the enterprise to take full advantages of the limited network resources and guarantee the best performance.

PLANET WGSW-24000 offers comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms comprised of port-based 802.1x user and device authentication. The administrators can now construct highly secured corporate networks with time and effort considerably less than before.

With its built-in web-based management, the PLANET WGSW-24000 offers an easy-to-use, platform-independent management and configuration facility. The PLANET WGSW-24000 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, the WGSW-24000 can also be accessed via Telnet and the console port. For secure remote management, the WGSW-24000 support SSL and SSH connection which encrypt the packet content at each session.

2.1.2 Switch Front Panel

Figure 2-1 shows the front panel of the switch.

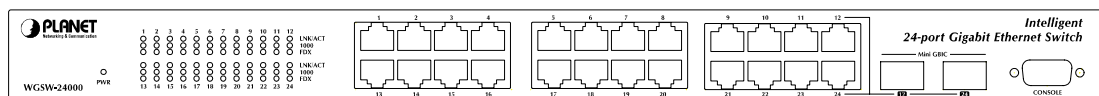


Figure 2-1 WGSW-24000 front panel.

2.1.3 LED Indications

Network:

LED	Color	Function
PWR	Green	Lights to indicate that the Switch is powered on.
LNK/ACT	Green	Lights to indicate the link through that port is successfully established.
100	Green	Lights to indicate the port is running in 100Mbps speed.
FDX/COL	Green	Blink to indicate the switch is actively sending or receiving data over that port.

Gigabit:

LED	Color	Function
LNK/ACT	Green	Lights to indicate the link through that port is successfully established.
1000	Green	Lights to indicate the port is running in 100Mbps speed.
FDX/COL	Green	Blink to indicate the switch is actively sending or receiving data over that port.

2.1.4 Switch Rear Panel

Figure 2-2 shows the rear panel of the switch

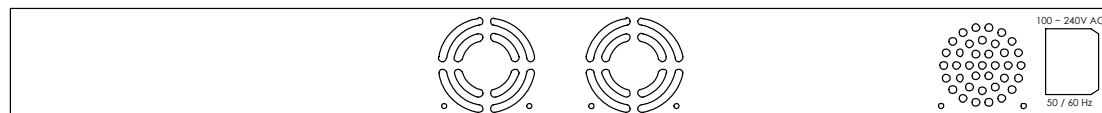


Figure 2-2 WGSW-24000 rear panel.

Power Notice:

1. The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.
2. In some area, installing a surge suppression device may also help to protect your switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the Switch

This section describes how to install the Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.2.1 Desktop Installation

To install the Switch on desktop or shelf, please follows these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the switch.

Step2: Place the switch on the desktop or the shelf near an AC power source.

Step3: Keep enough ventilation space between the switch and the surrounding objects.

Note: When choosing a location, please keep in mind the environmental restrictions discussed in

Chapter 1, Section 4, in Specification.

Step4: Connect the Switch to network devices.

- A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Switch
- B. Connect the other end of the cable to the network devices such as printer servers, workstations or routers...etc.

Note: Connection to the Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the switch.

- A. Connect one end of the power cable to the switch.
- B. Connect the power plug of the power cable to a standard wall outlet.

When the switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the switch in a 19-inch standard rack, please follows the instructions described below.

Step1: Place the switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the switch with supplied screws attached to the package.

Figure 2-5 shows how to attach brackets to one side of the switch.

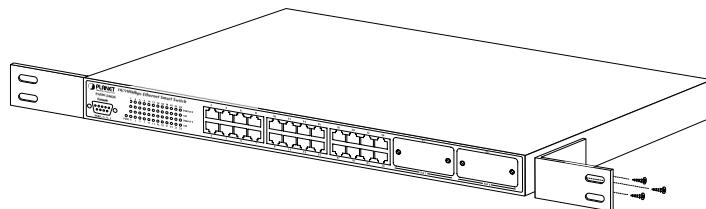


Figure 2-5 Attach brackets to the switch.

Caution:

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6

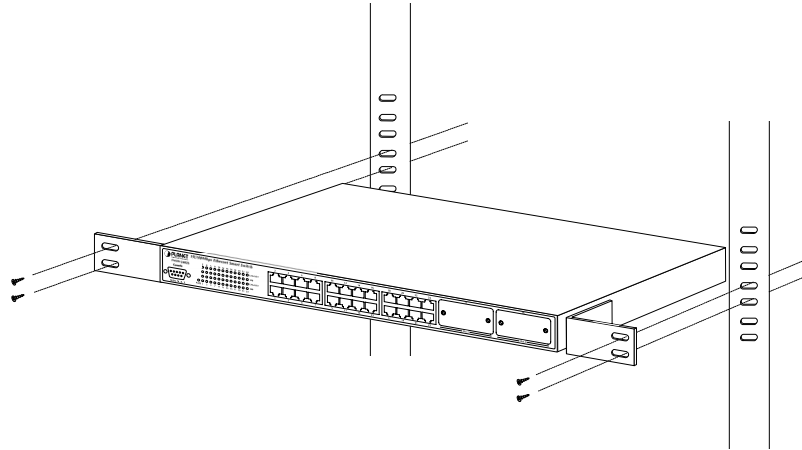


Figure 2-6 Mounting the Switch in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the switch.

3. CONFIGURATION

This chapter explains the methods that you can use to configure management access to the switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (work-station or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Management Access Overview
- Key Concepts
- Key Guidelines for Implementation
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Management Access Overview

The switch gives you the flexibility to access and manage the switch using any or all of the following methods:

- An administration console
- Web browser interface
- An external SNMP-based network management application

The administration console and Web browser interface support are embedded in the switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Console	<ul style="list-style-type: none">• No IP address or subnet needed• Text-based• Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems• Secure	<ul style="list-style-type: none">• Must be near switch or use dial-up connection• Not convenient for remote users• Modem connection may prove to be unreliable or slow
Web Browser	<ul style="list-style-type: none">• Ideal for configuring the switch remotely• Compatible with all popular browsers• Can be accessed from any location	<ul style="list-style-type: none">• Security can be compromised (hackers need only know the IP address and subnet mask)

	<ul style="list-style-type: none"> • Most visually appealing 	<ul style="list-style-type: none"> • May encounter lag times on poor connections
SNMP Agent	<ul style="list-style-type: none"> • Communicates with switch functions at the MIB level • Based on open standards 	<ul style="list-style-type: none"> • Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1 Management Methods Comparison

3.1.1 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console (serial) port.

There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 4 Command Line Interface Console Management**.

3.1.2 Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console (serial) port. When using this management method, a null-modem cable is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- 115,200 bps
- 8 data bits
- No parity
- 1 stop bit

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.2 Web Management

The switch provides a browser interface that lets you configure and manage the switch remotely. After

you set up your IP address for the switch, you can access the switch's Web interface applications directly in your Web browser by entering the IP address of the switch. You can then use your Web browser to list and manage switch configuration parameters from one central location, just as if you were directly connected to the switch's console port.

Web Management requires either Microsoft Internet Explorer 4.01 or later or Netscape Navigator 4.03 or later.

3.3 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the switch. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Network management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the switch are public.


3.4 Protocols

The switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.4.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the switch before you can establish access to it with a virtual terminal protocol.

 **Note:** Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.

3.4.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

3.4.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface

(MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent or Web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. COMMAND 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.

4.1 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.

4.1.1 Command

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

4.1.2 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.

4.1.3 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.

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.

4.1.4 Conventions

1. Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:
2. 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.
3. Empty strings ("") are not valid user defined strings.
4. 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).

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:	hexadecimal digit pairs

Table 4-1 Network Address Syntax

5. 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.
6. The value of '-----' designates that the value is unknown.

4.1.5 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
```

5. QUICK START UP

The CLI Quick Start up details procedures to quickly become acquainted with the software.

5.1 Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the software 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, we suggest 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.

5.2 System Info and System Setup

Quick Start up Software Version Information.

Command	Details
show hardware (in Privileged EXEC)	Allows the user to see the software version the device contains
	Machine Model (The type and number of ports the device provides.)
	For example: Machine Model..... 24+2G 24 = 24 10/100 ports 02 = 2 Uplink ports on back of switch

Table 5-1 Quick Start up Software Version Information.

Quick Star up Physical Port Data.

Command	Details
Show port all	Displays the Ports

(in Privileged EXEC)	
	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

Table 5-2 Quick Star up Physical Port Data.

Quick Start up Account Management

Command	Details
show users (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, the 'admin' user has Read/Write access and the 'guest' user has Read Only access. There can only be one Read/Write user and up to five Read Only users.
show login session (in User EXEC)	Displays all of the login session information
users passwd <username> (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.
copy system:running-config nvrn:startup-config (in Privileged EXEC)	This will save passwords and all other changes to the device. If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset
logout (in User EXEC and	Logs the user out of the switch

Privileged EXEC)	
------------------	--

Table 5-3 Quick Start up Account Management

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:** Helpful Hint: The user should do a “**copy system:running-config nvram:startup-config**”

after configuring the network parameters so that the configurations are not lost

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
	Locally Administered MAC Address - Can be configured to allow a locally administered MAC address
	MAC Address Type - Specifies which MAC address should be used for in-band connectivity
	Network Configurations Protocol Current - Indicates which network protocol is being used Default is 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

Table 5-4 Quick Start up IP Address

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

Command	Details
copy { nvram:startup-config nvram:errorlog nvram:msglog nvram:traplog} <url>	<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> <ul style="list-style-type: none"> ▫ xmodem:filepath/fileName
	<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>

Table 5-4 Quick Start up Uploading from Switch to Out-of-Band PC (XMODEM)

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

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

Table 5-5 Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)

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.

Command	Details
copy <url>	Sets the destination (download) data type to be an image (system:image)

<p>{nvram:startup-config system: image}</p>	<p>or a configuration file (nvram:startup-config).</p> <p>The URL must be specified as: ftp://ipAddr/filepath/fileName.</p> <p>The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.</p>
--	---

Table 5-6 Quick Start up Downloading from TFTP Server

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	<p>Enter yes when the prompt pops up that asks if you want to reset the system.</p> <p>This is the users choice either reset the switch or cold boot the switch, both work effectively.</p>

Table 5-7 Quick Start up Factory Defaults

6. 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 supports specific software commands.

- User Exec Mode
- Privileged Exec Mode
- Global Config Mode
- Vlan Mode
- Interface Config Mode
- Line Config Mode
- Policy Map Mode
- Policy Class Mode
- Class Map Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that 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.	(Switching) >	Enter Logout command
Privileged Exec Mode	From the User Exec Mode, enter the enable command.	(Switching) #	To exit this mode, enter exit or press Ctrl-Z.
VLAN Mode	From the Privileged User Exec mode, enter the vlan database command.	(Switching) (Vlan) #	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
Global Config Mode	From the Privileged Exec mode, enter the configure command.	(Switching) (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 <slot/port> command	(Switching) (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.	(Switching) (line) #	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.
Policy Map Mode	From the Global Configuration mode, enter the policy map <policy name> <in out> command.	(Switching) (Config-policy-map)#	To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.
Policy Class Mode	From the Policy Map mode enter the class-map <existed class-name> command.	(Switching) (Config-policy-classmap)#	To exit to Policy Map mode enter exit. To return to User Exec mode enter ctrl-Z.
Class Map Mode	From the Global Config mode, enter the class-map command.	(Switching) (Config-classmap)#	To exit to Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.

Table 6-1 Command Mode

6.1 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 12.

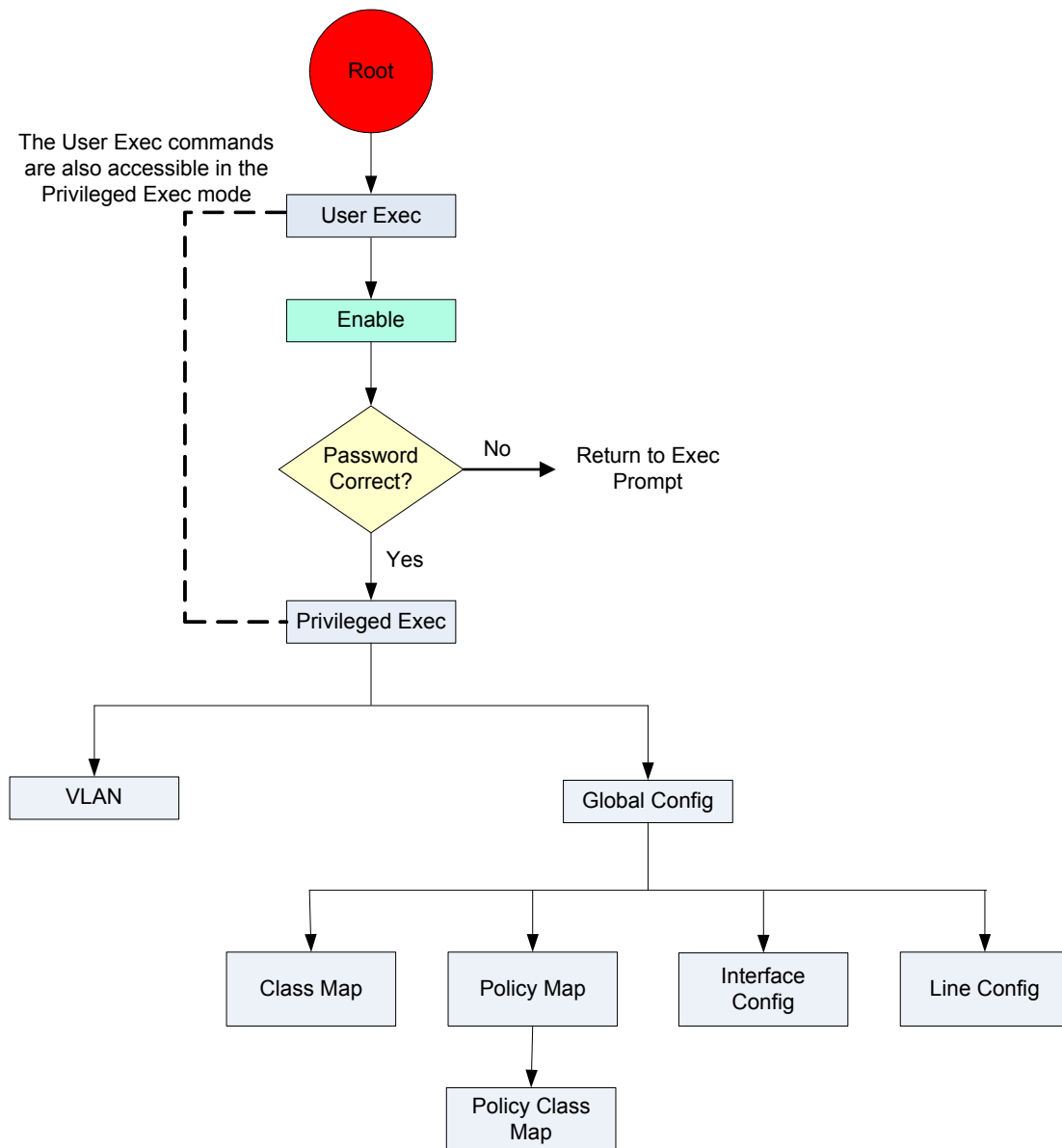


Figure 6-1 Mode-Based CLI

Accessing to all commands in the Privileged Exec mode and below is restricted through a password.

6.2 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: (Switching) >
```

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, enter the VLAN mode or enter the Global Configuration mode. The command prompt shown at this level is:

```
Command Prompt: (Switching) #
```

VLAN Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:

```
Command Prompt: (Switching) (VLAN) #
```

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 Configuration mode, the Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:

```
Command Prompt: (Switching) (Config) #
```

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

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: (Switching) (Interface <slot/port>)#
```

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

```
(Switching) (Config) # interface 2/1  
(Switching) (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: (Switching) (Line) #
```

Policy Map Mode

Use the `policy-map <policy-name>` command to access the QoS policy map configuration mode to configure the QoS policy map.

```
(Switching) (Config)# policy-map <policy-name>  
Command Prompt: (Switching) (Config policy-map) #
```

Policy Class Mode

Use the `class <class-name>` command to access the QoS policy-classmap mode to attach/remove a diffserv class to a policy and to configure the QoS policy map.

```
(Switching) (Config-policy-map) # class <class-name>  
Command Prompt: (Switching) (Config - policy-classmap) #
```

Class Map Mode:

This mode consists of class creation/deletion and matching commands. The class match commands specify layer 2, layer 3 and general match criteria. Use the `class-map class-map-name` commands to access the QoS class map configuration mode to configure QoS class maps.

```
(Switching) (Config)# class map <class-map-name>  
Command Prompt: (Switching) (Config - class) #
```

6.3 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:

```
(Switching) #show arp brief
                ^
% Invalid input detected at '^' marker.

(Switching) #
```

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.

6.4 "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.

6.4.1 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.

6.4.2 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 interface?) and (no inte?) cases of the "?", the options displayed are identical to the

case when the **"no"** token is not specified as in (interface) and (inte?).

7. CLI Commands: Base

This chapter provides detailed explanation of the Switching commands. The commands are divided into four 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 transfer or save 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

7.1 System Information and Statistics Commands

7.1.1 show arp switch

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


- **Format** show arp switch
- **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** A valid slot number and a valid port number.

7.1.2 show eventlog

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

- **Format** show eventlog
- **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.

7.1.3 show hardware

This command displays inventory information for the switch.

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

7.1.4 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** show interface {<slot/port> | switchport}
- **Mode** Privileged EXEC

The display parameters when the argument is '<slot/port>' are 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**' are 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.

7.1.5 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

- **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.
- **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.
- **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**' are 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.

7.1.6 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.

7.1.7 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.slot/port. The port which this address was learned.
- **if Index** - This object indicates the ifIndex of the interface table entry associated with this port.
- **Status** - The status of this entry. The meanings of the values are:
 - **Static** - The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.
 - **Learned** - The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.
 - **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.
 - **Self** - The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).
 - **GMRP Learned** - The value of the corresponding was learned via GMRP and applies to Multicast.
 - **Other** - The value of the corresponding instance does not fall into one of the other categories.

7.1.8 show msglog

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

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

- **Format** **show msglog**
- **Mode** **Privileged EXEC**
- **Message** - The message that has been logged.

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

7.1.9 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** `show running-config`
- **Mode** Privileged EXEC

7.1.10 show sysinfo

This command displays switch information.

- **Format** `show sysinfo`
- **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 alphanumeric 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.

7.1.11 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** `snmp-server {sysname <name> | location <loc> | contact <con>}`
- **Mode** Global Config

7.2 Management VLAN Commands

7.2.1 network mgmt_vlan

This command configures the Management VLAN ID.

- **Default** 1
- **Format** `network mgmt_vlan <1-4094>`
- **Mode** Privileged EXEC

7.3 Dot1P Commands

7.3.1 classofservice dot1pmapping

This command maps an 802.1p priority to an internal traffic class for a device when in 'Global Config' mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be the range from 0-7. The command is only available on platforms that support priority to traffic

class mapping on a 'per-port' basis, and the number of available traffic classes may vary with the platform.

- **Format** `classofservice dot1pmapping <userpriority> <trafficclass>`
- **Mode** **Global Config or Interface Config**

7.3.2 show classofservice dot1pmapping

This command displays the current 802.1p priority mapping to internal traffic classes for a specific interface. The slot/port parameter is required on platforms that support priority to traffic class mapping on a 'per-port' basis.

Platforms that support priority to traffic class mapping on a per-port basis:

- **Format** `show classofservice dot1pmapping <slot/port>`

Platforms that do not support priority to traffic class mapping on a per-port basis:

- **Format** `show classofservice dot1pmapping`
- **Mode** **Privileged EXEC and User EXEC**

7.3.3 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** `vlan port priority all <priority>`
- **Mode** **Global Config**

7.3.4 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** `vlan priority <priority>`
- **Mode** **Interface Config**

7.4 LAG/Port-Channel (802.3ad) Commands

7.4.1 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** `port-channel staticcapability`
- **Mode** **Global Config**

7.4.1.1 no port-channel staticcapability

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

- **Default** Disabled
- **Format** **no port-channel staticcapability**
- **Mode** **Global Config**

7.4.2 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** **show port-channel brief**
- **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.

7.5 Management Commands

These commands manage the switch and show current management settings.

7.5.1 bridge aging-time

This command configures the forwarding database address aging timeout in seconds. In an IVL system, the [fdbid/all] parameter is required.

- **Default** 300
- **Format** **bridge aging-time <10-1,000,000> [fdbid | all]**
- **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.

7.5.1.1 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.

- **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.

7.5.2 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**

7.5.2.1 no mtu

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

- **Format** **no mtu**
- **Mode** **Interface Config**

7.5.3 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**

7.5.3.1 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**

7.5.4 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**

7.5.5 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**

7.5.5.1 no network mac-type

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

Format **no network mac-type**

Mode **Privileged EXEC**

7.5.6 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**

7.5.7 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**

7.5.8 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**

7.5.8.1 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**

7.5.9 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**

7.5.9.1 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**

7.5.10 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**

7.5.10.1 no serial baudrate

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

- **Format** **no serial baudrate**
- **Mode** **Line Config**

7.5.11 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**

7.5.11.1 no serial timeout

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

- **Format** **no serial timeout**
- **Mode** **Line Config**

7.5.12 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**

7.5.13 show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

- **Default** **all**
- **Format** **show forwardingdb agetime [fdbid | all]**
- **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.

Agetime Displays the address aging timeout for the associated forwarding database in IVL.

5.7.14 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** **show network**
- **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 BridgIdentifier 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.

7.5.15 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. This 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.

7.5.16 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.

7.5.17 show snmpcommunity

This command displays SNMP community information.

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

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

- **Format** **show snmpcommunity**
- **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.

7.5.18 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.

7.5.19 show trapflags

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

- **Format** `show trapflags`
- **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.

7.5.20 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** **snmp-server community <name>**
- **Mode** **Global Config**

7.5.20.1 no snmp-server community

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

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

7.5.21 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** **snmp-server community ipaddr <ipaddr> <name>**
- **Mode** **Global Config**

7.5.21.1 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** **no snmp-server community ipaddr <name>**
- **Mode** **Global Config**

7.5.22 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** `snmp-server community ipmask <ipmask> <name>`
- **Mode** `Global Config`

7.5.22.1 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** `no snmp-server community ipmask <name>`
- **Mode** `Global Config`

7.5.23 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** `snmp-server community mode <name>`
- **Mode** `Global Config`

7.5.23.1 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`

7.5.24 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`

7.5.25 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`

7.5.26 snmp-server enable traps

This command enables the Authentication Flag.

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

7.5.26.1 no snmp-server enable traps

This command disables the Authentication Flag.

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

7.5.27 snmp-server enable traps bcaststorm

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**

7.5.27.1 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**

7.5.28 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**

7.5.28.1 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**

7.5.29 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**

7.5.29.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

- **Format** **no snmp-server enable traps multiusers**
- **Mode** **Global Config**

7.5.30 snmp-server enable traps stpmode

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

- **Default** **Enabled**
- **Format** **snmp-server enable traps stpmode**
- **Mode** **Global Config**

7.5.30.1 no snmp-server enable traps stpmode

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

- **Format** **no snmp-server enable traps stpmode**
- **Mode** **Global Config**

7.5.31 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** **snmptrap <name> <ipaddr>**
- **Mode** **Global Config**


7.5.31.1 no snmptrap

This command deletes trap receivers for a community.

- **Format** **no snmptrap <name> <ipaddr>**
- **Mode** **Global Config**

7.5.32 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> <ipaddroid> <ipaddrnew>**

- **Mode** **Global Config**

7.5.33 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**

7.5.33.1 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**

7.5.34 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**

7.5.34.1 no telnet


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

- **Format** **no telnet**
- **Mode** **Privileged EXEC**

7.6 Device Configuration Commands

7.6.1 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** **addport <logical slot/port>**
- **Mode** **Interface Config**

7.6.2 auto-negotiate

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

- **Format** auto-negotiate
- **Mode** Interface Config

7.6.2.1 no auto-negotiate

This command disables automatic negotiation on a port.

- **Format** no auto-negotiate
- **Mode** Interface Config

7.6.3 auto-negotiate all

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

- **Format** auto-negotiate all
- **Mode** Global Config

7.6.3.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

- **Format** no auto-negotiate all
- **Mode** Global Config

7.6.4 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** delete interface { <logical slot/port> | all}
- **Mode** Interface Config

7.6.5 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** deleteport <logical slot/port>
- **Mode** Interface Config

7.6.6 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>.

The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

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

The <vlanid> parameter must identify a valid VLAN.

Up to 100 static MAC filters may be created.

- **Format** **macfilter <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.6.1 no macfilter

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.7 macfilter adddest

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter adddest <macaddr> <vlanid>**
- **Mode** **Interface Config**

7.6.7.1 no macfilter adddest

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter adddest <macaddr> <vlanid>**
- **Mode** **Interface Config**

7.6.8 macfilter adddest all

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter adddest all <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.8.1 no macfilter adddest all

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter adddest all <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.9 macfilter addsrc

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter addsrc <macaddr> <vlanid>**
- **Mode** **Interface Config**

7.6.9.1 no macfilter addsrc

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter addsrc <macaddr> <vlanid>**
- **Mode** **Interface Config**

7.6.10 macfilter addsrc all

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter addsrc all <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.10.1 no macfilter addsrc all

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

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter addsrc all <macaddr> <vlanid>**
- **Mode** **Global Config**

7.6.11 monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). The first slot/port is the source monitored port and the second slot/port is the destination probe port. If this command is executed while port monitoring is enabled, it will have the effect of changing the probe and monitored port values.

- **Format** **monitor session source <slot/port> destination <slot/port>**
- **Mode** **Global Config**

7.6.11.1 no monitor session

This command removes the monitor session (port monitoring) designation from both the source probe port and the destination monitored port and removes the probe port from all VLANs. The port must be manually re-added to any desired VLANs.

- **Format** **no monitor session**
- **Mode** **Global Config**

7.6.12 monitor session mode

This command configures the monitor session (port monitoring) mode to enable. The probe and monitored ports must be configured before monitor session (port monitoring) can be enabled. If enabled, the probe port will monitor all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

- **Default** **Disabled**
- **Format** **monitor session mode**
- **Mode** **Global Config**

7.6.12.1 no monitor session mode

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

- **Format** **no monitor session mode**
- **Mode** **Global Config**

7.6.13 port lacpmode

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

- **Default** **Disabled**
- **Format** **port lacpmode**
- **Mode** **Interface Config**

7.6.13.1 no port lacpmode

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

- **Format** **no port lacpmode**

- **Mode** **Interface Config**

7.6.14 port lacpmode all

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

- **Format** **port lacpmode all**
- **Mode** **Global Config**


7.6.14.1 no port lacpmode all

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

- **Format** **no port lacpmode all**
- **Mode** **Global Config**

7.6.15 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**

7.6.16 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**

7.6.16.1 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**

7.6.17 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**

7.6.17.1 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**

7.6.18 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**

7.6.19 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**

7.6.19.1 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**

7.6.20 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>
- **Mode** Interface Config

7.6.20.1 no protocol vlan group

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

- **Format** no protocol vlan group <groupid>
- **Mode** Interface Config

7.6.21 protocol vlan group all

This command adds all physical interfaces 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 all <groupid>
- **Mode** Global Config

7.6.21.1 no protocol vlan group all

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

- **Format** no protocol vlan group all <groupid>
- **Mode** Global Config

7.6.22 set garp timer join

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

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

- **Default** 20 centiseconds (0.2 seconds)
- **Format** set garp timer join <10-100>
- **Mode** Interface Config

7.6.22.1 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**

7.6.23 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**

7.6.23.1 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**

7.6.24 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** **set garp timer leave <20-600>**
- **Mode** **Interface Config**

7.6.24.1 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** **no set garp timer leave**
- **Mode** **Interface Config**

7.6.25 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** **set garp timer leave all <20-600>**
- **Mode** **Global Config**

7.6.25.1 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** **no set garp timer leave all**
- **Mode** **Global Config**

7.6.26 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** **set garp timer leaveall <200-6000>**
- **ModeInterface** **Config**

7.6.26.1 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** **no set garp timer leaveall**
- **Mode** **Interface Config**

7.6.27 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** **set garp timer leaveall all <200-6000>**
- **Mode** **Global Config**

7.6.27.1 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**

7.6.28 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**

7.6.28.1 no set gmrp adminmode

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

- **Format** **no set gmrp adminmode**
- **Mode** **Privileged EXEC**

7.6.29 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 portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Default** Disabled
- **Format** **set gmrp interfacemode**
- **Mode** **Interface Config**

7.6.29.1 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 portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Format** **no set gmrp interfacemode**
- **Mode** **Interface Config**

7.6.30 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 portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Default** Disabled
- **Format** **set gmrp interfacemode all**
- **Mode** **Global Config**

7.6.30.1 no set gmrp interfacemode all

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

- **Format** **no set gmrp interfacemode all**
- **Mode** **Global Config**

7.6.31 set gvrp adminmode

This command enables GVRP.

- **Default** Disabled
- **Format** **set gvrp adminmode**
- **Mode** **Privileged EXEC**

7.6.31.1 no set gvrp adminmode

This command disables GVRP.

- **Format** **no set gvrp adminmode**
- **Mode** **Privileged EXEC**

7.6.32 set gvrp interfacemode

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

- **Default** **Disabled**
- **Format** **set gvrp interfacemode**
- **Mode** **Interface Config**

7.6.32.1 no set gvrp interfacemode

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

- **Format** **no set gvrp interfacemode**
- **Mode** **Interface Config**

7.6.33 set gvrp interfacemode all

This command enables GVRP (GARP VLAN Registration Protocol) for all ports.

- **Default** **Disabled**
- **Format** **set gvrp interfacemode all**
- **Mode** **Global Config**

7.6.33.1 no set gvrp interfacemode all

This command disables GVRP (GARP VLAN Registration Protocol) for all ports. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

- **Format** **no set gvrp interfacemode all**
- **Mode** **Global Config**

7.6.34 show description

This command displays the port description information for one or all interfaces.

- **Format** **show description {<slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

7.6.35 show garp

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

- **Format** **show garp**
- **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.

7.6.36 show gmrp configuration

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

- **Format** **show gmrp 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.

7.6.37 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.

7.6.38 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.

7.6.39 show mac-address-table gmrp

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

- **Format** **show mac-address-table gmrp**
- **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.
- **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:).

7.6.40 show mac-address-table igmpsnooping

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

- **Format** **show mac-address-table igmpsnooping**
- **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.
- **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:).

7.6.41 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** **show mac-address-table multicast [<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.
- **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.

7.6.42 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** `show mac-address-table static {<macaddr> <vlanid> | all}`
- **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).

7.6.43 show mac-address-table staticfiltering

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

- **Format** `show mac-address-table staticfiltering`
- **Mode** **Privileged EXEC**
- **Mac Address** - An 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.
- **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:).

7.6.44 show mac-address-table stats

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

- **Format** `show mac-address-table stats`
- **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.

7.6.45 show monitor

This command displays the Port monitoring information for the system.

- **Format** `show monitor`
- **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.

7.6.46 show port

This command displays port information.

- **Format** `show port {<slot/port> | all}`
- **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.

7.6.47 show port protocol

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

- **Format** `show port protocol {<groupid> | all}`
- **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.

7.6.48 show port-channel

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

- **Format** `show port-channel {<logical slot/port> | all}`
- **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 portchannel (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).

7.6.49 show storm-control

This command displays switch configuration information.

- **Format** **show storm-control**
- **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.

7.6.50 show vlan

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

- **Format** **show vlan <vlanid>, 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.

7.6.51 show vlan brief

This command displays a list of all configured VLANs.

- **Format** **show vlan brief**
- **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 Namev** - 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).

7.6.52 show vlan port

This command displays VLAN port information.

- **Format** **show vlan port {<slot/port> | all}**
- **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.

7.6.53 shutdown

This command disables a port.

- **Default** **Enabled**
- **Format** **shutdown**
- **Mode** **Interface Config**

7.6.53.1 no shutdown

This command enables a port.

- **Format** **no shutdown**
- **Mode** **Interface Config**

7.6.54 shutdown all

This command disables all ports.

- **Default** **Enabled**
- **Format** **shutdown all**
- **Mode** **Global Config**

7.6.54.1 no shutdown all

This command enables all ports.

- **Format** **no shutdown all**
- **Mode** **Global Config**

7.6.55 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 'snmpserverenable traps linkmode' command.

- **Format** **snmp trap link-status**
- **Mode** **Interface Config**

7.6.55.1 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 'snmpserver enable traps linkmode' command).

- **Format** **no snmp trap link-status**
- **Mode** **Interface Config**

7.6.56 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 "snmpserver enable traps linkmode").

- **Format** **snmp trap link-status all**
- **Mode** **Global Config**

7.6.56.1 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 "snmpserver enable traps linkmode").

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

7.6.57 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

7.6.58 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**

7.6.58.1 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**

7.6.59 description

This command sets the description information for the interface. The description is an alphanumeric

string of up to 64 characters. To use spaces as part of a description, enclose it in double quotes like: "Port 1 connect to Ln 1"

- **Format** **description <description>**
- **ModeInterface Config**

7.6.60 speed

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

- **Format** **speed {{100 | 10} {half-duplex | full-duplex} | 1000 fullduplex}**
- **ModeInterface Config**

Acceptable values are:

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

7.6.61 speed all

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

- **Format** **speed all {{100 | 10} {half-duplex | full-duplex} | 1000 fullduplex}**
- **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

7.6.62 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.

- **Format** **storm-control broadcast**
- **Mode** **Global Config**

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

1000M	5	2
-------	---	---

Table 7-1 Broadcast Storm Recovery Thresholds

7.6.62.1 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.

- **Format** **no storm-control broadcast**
- **Mode** **Global Config**

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

7.6.63 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**

7.6.63.1 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**

7.6.64 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**

7.6.64.1 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**

7.6.65 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** **Admit All**
- **Format** **vlan acceptframe {vlanonly | all}**
- **Mode** **Interface Config**

7.6.65.1 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** **vlan acceptframe {vlanonly | all}**
- **Mode** **Interface Config**

7.6.66 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** **Disabled**
- **Format** **vlan ingressfilter**
- **Mode** **Interface Config**

7.6.66.1 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** **no vlan ingressfilter**
- **Mode** **Interface Config**

7.6.67 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**

7.6.68 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**

7.6.68.1 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**

7.6.69 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.

7.6.70 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** **vlan participation all {exclude | include | auto} <1-4094>**

- **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.

7.6.71 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** **vlan port acceptframe all {vlanonly | all}**
- **Mode** **Global Config**

7.6.71.1 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** **no vlan port acceptframe all {vlanonly | all}**
- **Mode** **Global Config**

7.6.72 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** **vlan port ingressfilter all**
- **Mode** **Global Config**

7.6.72.1 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** **no vlan port ingressfilter all**
- **Mode** **Global Config**

7.6.73 vlan port pvid all

This command changes the VLAN ID for all interfaces.

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

7.6.73.1 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**

7.6.74 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**

7.6.74.1 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**

7.6.75 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**

7.6.76 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

7.6.76.1 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

7.6.77 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

7.6.78 vlan pvid

This command changes the VLAN ID per interface.

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

7.6.78.1 no vlan pvid

This command sets the VLAN ID per interface to 1.

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

7.6.79 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

7.6.79.1 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**

7.7 User Account Management Commands

These commands manage user accounts.

7.7.1 disconnect

This command closes a telnet session.

- **Format** **disconnect {<sessionID> | all}**
- **Mode** **Privileged EXEC**

7.7.2 show loginsession

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

- **Format** **show loginsession**
- **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.

7.7.3 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, the '**admin**' user has Read/Write access and the '**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 Read-Write, 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.

7.7.4 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**

7.7.4.1 no users name

This command removes an operator.

- **Format** **no users name <username>**
- **Mode** **Global Config**

 **Note:** The 'admin' user account cannot be deleted.

7.7.5 users passwd

This command is used to change a password. The password should not be more than eight alphanumeric characters in length. If a user is authorized for authentication or encryption is enabled, the password must be at least eight alphanumeric characters in length. The username and password are not case sensitive when a password is changed, a prompt will ask for the former password. If none, press enter.

- **Default** **No Password**
- **Format** **users passwd <username>**
- **Mode** **Global Config**

7.7.5.1 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** **no users passwd <username>**
- **Mode** **Global Config**

7.7.6 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** **readwrite for 'admin' user; readonly for all other users**
- **Format** **users snmpv3 accessmode <username> {readonly | readwrite}**
- **Mode** **Global Config**

7.7.6.1 no users snmpv3 accessmode

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

- **Format** **no users snmpv3 accessmode <username>**
- **Mode** **Global Config**

7.7.7 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 is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The <username> is the login user name associated with the authentication protocol.

- **Default** **no authentication**
- **Format** **users snmpv3 authentication <username> {none | md5 | sha}**
- **Mode** **Global Config**

7.7.7.1 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**

7.7.8 users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are des or none.

If des is specified, the required key may 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. When using the des protocol, the user login password is also used as the snmpv3 encryption password and therefore must be at least eight characters in length.

If none is specified, a key must not be provided. The <username> is the login user name associated with the specified encryption.

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

7.7.8.1 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**

7.8 System Utilities

This section describes system utilities.

7.8.1 clear config

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

- **Format** **clear config**
- **Mode** **Privileged EXEC**

7.8.2 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**

7.8.3 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**

7.8.4 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**

7.8.5 clear port-channel

This command clears all port-channels (LAGs).

- **Format** **clear port-channel**
- **Mode** **Privileged EXEC**

7.8.6 clear traplog

This command clears the trap log.

- **Format** **clear traplog**
- **Mode** **Privileged EXEC**

7.8.7 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

- **Format** **clear vlan**
- **Mode** **Privileged EXEC**

7.8.8 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 configuration (**nvrām:startup-config**), error log (**nvrām:errorlog**), message log (**nvrām:msglog**) and trap log (**nvrām:traplog**). A URL is specified for the destination.

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

The command can be used to save the running configuration to **nvrām** by specifying the source as **system:running-config** and the destination as **nvrām:startup-config**

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

- **Default** none
- **Format** **copy nvrām:startup-config <url>**
 - copy nvrām:errorlog <url>**
 - copy nvrām:msglog <url>**
 - copy nvrām:traplog <url>**
 - copy <url> nvrām:startup-config**
 - copy <url> system:image**


```
copy system:running-config nvram:startup-config
```

```
copy <url> nvram:sslpem-root
```

```
copy <url> nvram:sslpem-server
```

```
copy <url> nvram:sslpem-dhweak
```

```
copy <url> nvram:sslpem-dhstrong
```

```
copy <url> nvram:sshkey-rsa1
```


```
copy <url> nvram:sshkey-rsa2
```

```
copy <url> nvram:sshkey-dsa
```

- **Mode** Privileged EXEC

7.8.9 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

7.8.10 ping

This command checks if another computer is on the network which is listening for connections. To use this command, configure the switch for network (in-band) connection. 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

7.8.11 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

8. CLI COMMANDS: QUALITY OF SERVICE

This chapter provides a detailed explanation of the Quality of Service (QOS) commands. The following QOS CLI commands are available in the software QOS Package.

The commands are divided into these different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

8.1 CLI Commands: Access Control List

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

8.1.1 show ip access-lists

This command displays an Access Control List (ACL) and all of the rules that are defined for the ACL.

The <accesslistnumber> is the number used to identify the ACL.

- **Format** **show ip access-lists <accesslistnumber>**
- **Mode** **Privileged EXEC and User EXEC**
- **Rule Number** - This displays the number identifier for each rule that is defined for the ACL.
- **Action** - This displays the action associated with each rule. The possible values are Permit or Deny.
- **Protocol** - This displays the protocol to filter for this rule.
- **Source IP Address** - This displays the source IP address for this rule.
- **Source IP Mask** - This field displays the source IP Mask for this rule.
- **Source Ports** - This field displays the source port range for this rule.
- **Destination IP Address** - This displays the destination IP address for this rule.
- **Destination IP Mask** - This field displays the destination IP Mask for this rule.
- **Destination Ports** - This field displays the destination port range for this rule.
- **Service Type Field Match** - This field indicates whether an IP DSCP, IP Precedence, or IP TOS match condition is specified for this rule.
- **Service Type Field Value** - This field indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence, or IP TOS).

8.2 Configuration Commands

8.2.1 access-list

This command creates an Access Control List (ACL) that is identified by the parameter

<accesslistnumber>. The ACL number is an integer from 1 to 199. The range 1 to 99 is for normal ACL List and 100 to 199 is for extended ACL List. The ACL rule is created with the option of permit or deny. The protocol to filter for an ACL rule is specified by giving the protocol to be used like cmp, igmp, ip, tcp, udp. The command specifies a source ipaddress and source mask for match condition of the ACL rule specified by the srcip and srcmask parameters. The source layer 4 port match condition for the ACL rule are specified by the port value parameter. The <startport> and <endport> parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the destination port range. The <portvalue> parameter uses a single keyword notation and currently has the values of domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range. The command specifies a destination ipaddress and destination mask for match condition of the ACL rule specified by the dstip and dstmask parameters. The command specifies the TOS for an ACL rule depending on a match of precedence or DSCP values using the parameters tos, tosmask, dscp.

- **Default** none
- **Format** `access-list {(<1-99> {deny | permit} <srcip> <srcmask>) | (<100-199> {deny | permit} {evry | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask> [{eq {<portkey> | <portvalue>} | range <startport> <endport>}] <dstip> <dstmask> [{eq {<portkey> | <portvalue>} | range <startport> <endport>}]} [precedence <precedence>] [tos <tos> <tosmask>] [dscp <dscp>]]}}`
- **Mode** Global Config

8.2.1.1 no access-list

This command deletes an ACL that is identified by the parameter <accesslistnumber> from the system.

- **Format** `no access-list <accesslistnumber>`
- **Mode** Global Config

8.2.2 ip access-group

This command attaches a specified access-control list to an interface.

- **Default** none
- **Format** `ip access-group <accesslistnumber> [in | out]`
- **Mode** Interface Config

8.2.3 ip access-group all

This command attaches a specified access-control list to all interfaces.

- **Default** none
- **Format** `ip access-group all <accesslistnumber> [in | out]`

- **Mode** **Global Config**

8.3 CLI Commands: Differentiated Services

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

The user configures DiffServ in several stages by specifying:

1. Class

- creating and deleting classes
- defining match criteria for a class. Note: The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

2. Policy

- creating and deleting policies
- associating classes with a policy
- defining policy statements for a policy/class combination

3. Service

- adding and removing a policy to/from a directional (i.e., inbound, outbound) interface

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class.

The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

Packet processing begins by testing the match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

Note that the type of class - all, any, or acl - has a bearing on the validity of match criteria specified when defining the class. A class type of 'any' processes its match rules in an ordered sequence; additional rules specified for such a class simply extend this list. A class type of 'acl' obtains its rule list by interpreting each ACL rule definition at the time the Diffserv class is created. Differences arise when specifying match criteria for a class type 'all', since only one value for each non-excluded match field is allowed within a class definition. If a field is already specified for a class, all subsequent attempts to specify the same field fail, including the cases where a field can be specified multiple ways through alternative formats. The exception to this is when the 'exclude' option is specified, in which case this restriction does not apply to the excluded fields.

The following class restrictions are imposed by the DiffServ design:

- nested class support limited to:
 - 'any' within 'any'
 - 'all' within 'all'
 - no nested 'not' conditions
 - no nested 'acl' class types
 - each class contains at most one referenced class
- hierarchical service policies not supported in a class definition
- access list matched by reference only, and must be sole criterion in a class

- i.e., ACL rules copied as class match criteria at time of class creation, with class type 'any'
- implicit ACL 'deny all' rule also copied
- no nesting of class type 'acl'

Regarding nested classes, referred to here as class references, a given class definition can contain at most one reference to another class, which can be combined with other match criteria. The referenced class is truly a reference and not a copy, since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes otherwise the change is rejected. A class reference may be removed from a class definition.

The user can display summary and detailed information for classes, policies and services. All configuration information is accessible via the CLI, Web, and SNMP user interfaces.

8.3.1 diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

- **Format** **diffserv**
- **Mode** **Global Config**

8.3.1.1 no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

- **Format** **no diffserv**
- **Mode** **Global Config**

8.4 Class Commands

The 'class' command set is used in DiffServ to define:

- **Traffic Classification** - Specify Behavior Aggregate (BA), based on DSCP, and Multi-Field (MF) classes of traffic (name, match criteria)
- **Service Levels** - Specify the BA forwarding classes / service levels. Conceptually, DiffServ is a twolevel hierarchy of classes: 1. Service/PHB, 2. Traffic Class

This set of commands consists of class creation/deletion and matching, with the class match commands specifying layer 3, layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic belonging to the class. Note that once a class match criterion is created for a class, it cannot be changed or deleted - the entire class must be deleted and re-created.

The CLI command root is **class-map**.

8.4.1 class-map


This command defines a new DiffServ class of type **match-all**, **match-any** or **match-access-group**. The **<classname>** parameter is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (Note: the class name 'default' is reserved and must not be used here).

When used without any match condition, this command enters the class-map mode. The **<classname>** is the name of an existing DiffServ class (note: the class name 'default' is reserved and is not allowed here)

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.

The class type of **match-any** indicates only one of the match criteria must be true for a packet to belong to the class; multiple matching criteria are evaluated in a sequential order, with the highest precedence awarded to the first criterion defined for the class.

The class type of **match-access-group** indicates the individual class match criteria are evaluated based on an access list (ACL). The **<aclid>** parameter is an integer specifying an existing ACL number (refer to the appropriate ACL documentation for the valid ACL number range). A **match-access-group** class type copies its set of match criteria from the current rule definition of the specified ACL number. All elements of a single ACL Rule are treated by DiffServ as a grouped set, similar to class type all. For any class, at least one class match condition must be specified for the class to be considered valid.

 **Note:** The class match conditions are obtained from the referenced access list at the time of class creation. Thus, any subsequent changes to the referenced ACL definition do not affect the DiffServ class. To pick up the latest ACL definition, the DiffServ class must be deleted and re-created.

This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

 **Note:** The CLI mode is changed to Class-Map Config when this command is successfully executed.

- **Format** **class-map** [{**match-all** | **match-any** | **match-access-group** **<aclid>**}]
 <classmapname>
- **Mode** **Global Config**

8.4.1.1 no class-map

This command eliminates an existing DiffServ class. The **<classname>** is the name of an existing DiffServ class (note: the class name 'default' is reserved and is not allowed here). This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, this deletion attempt shall fail.

- **Format** **no class-map** **<classname>**
- **Mode** **Global Config**

8.4.2 class-map rename

This command changes the name of a DiffServ class. The <classname> is the name of an existing DiffServ class. The <newclassname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (Note: the class name 'default' is reserved and must not be used here).

- **Default** **None**
- **Format** **class-map rename <classname> <newclassname>**
- **Mode** **Global Config**


8.4.3 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. The optional [not] parameter has the effect of negating this match condition for the class (i.e., none of the packets are considered to belong to the class).

- **Default** **None**
- **Format** **match [not] any**
- **Mode** **Class-Map Config**

8.4.4 match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The <refclassname> is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

 **Note:** There is no [not] option for this match command.

- **Default** **None**
- **Format** **match class-map <refclassname>**
- **Mode** **Class-Map Config**

Restrictions - The class types of both <classname> and <refclassname> must be identical (i.e., any vs. any, or all vs. all). A class type of acl is not supported by this command. Cannot specify <refclassname> the same as <classname> (i.e., self-referencing of class name not allowed).

At most one other class may be referenced by a class.

Any attempt to delete the <refclassname> class while still referenced by any <classname> shall fail.

The combined match criteria of <classname> and <refclassname> must be an allowed combination based on the class type. Any subsequent changes to the <refclassname> class match criteria must maintain this validity, or the change attempt shall fail.

The total number of class rules formed by the complete reference class chain (includes both predecessor and successor classes) must not exceed a platform-specific maximum.

In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

8.4.4.1 no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The <refclassname> is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition. Note: there is no [not] option for this match command.

- **Default** **None**
- **Format** **no match class-map <refclassname>**
- **Mode** **Class-Map Config**

8.4.5 match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The <macaddr> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask> parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination MAC addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] destination-address mac <macaddr> <macmask>**
- **Mode** **Class-Map Config**

8.4.6 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The <ipaddr> parameter specifies an IP address. The <ipmask> parameter specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination IP addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] dstip <ipaddr> <ipmask>**
- **Mode** **Class-Map Config**

8.4.7 match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

To specify the match condition as a single keyword, the value for <portkey> is one of the supported port name keywords. The currently supported <portkey> values are: **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **fttp**, **www**. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.


To specify the match condition using a numeric range notation, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.


The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination layer 4 port numbers except for the one specified here).

- **Default** **None**
- **Format** **match [not] dstl4port {<portkey> | <0-65535> [<0-65535>]}**
- **Mode** **Class-Map Config**

8.4.8 match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked). The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all IP DSCP values except for what is specified here). The **<dscpval>** value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef**.


 **Note:** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.


 **Note:** To specify a match on all DSCP values, use the match [not] ip tos <tosbits> <tosmask> command with **<tosbits>** set to 0 and **<tosmask>** set to 03 (hex).

- **Default** **None**
- **Format** **match [not] ip dscp <dscpval>**
- **Mode** **Class-Map Config**

8.4.9 match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all IP Precedence values except for what is specified here).


 **Note:** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.


 **Note:** To specify a match on all Precedence values, use the match [not] ip tos <tosbits> <tosmask> command with <tosbits> set to 0 and <tosmask> set to 1F (hex).

- **Default** **None**
- **Format** **match [not] ip precedence <0-7>**
- **Mode** **Class-Map Config**

8.4.10 match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of <tosbits> is a two-digit hexadecimal number from 00 to ff. The value of <tosmask> is a two-digit hexadecimal number from 00 to ff. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all IP Precedence values except for what is specified here). The <tosmask> denotes the bit positions in <tosbits> that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a <tosbits> value of a0 (hex) and a <tosmask> of a2 (hex).

 **Note:** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

 **Note:** In essence, this is the "free form" version of the IP DSCP/Precedence/TOS match specification in that the user has complete control of specifying which bits of the IP Service Type field are checked.

- **Default** **None**
- **Format** **match [not] ip tos <tosbits> <tosmask>**
- **Mode** **Class-Map Config**

8.4.11 match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for <protocol-name> is one of the supported protocol name keywords. The currently supported values are: **icmp, igmp, ip, tcp, udp**.

Note that a value of **ip** is interpreted to match all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Note: This command does not validate the protocol number value against the current list defined by IANA.

The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all IP Protocol numbers except for the one specified here).

- **Default** **None**

- **Format** **match [not] protocol {<protocol-name> | <0-255>}**
- **Mode** **Class-Map Config**

8.4.12 match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The **<address>** parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The **<macmask>** parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source MAC addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] source-address mac <address> <macmask>**
- **Mode** **Class-Map Config**

8.4.13 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The **<ipaddr>** parameter specifies an IP address. The **<ipmask>** parameter specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous. The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source IP addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] srcip <ipaddr> <ipmask>**
- **Mode** **Class-Map Config**

8.4.14 match srcI4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

To specify the match condition as a single keyword notation, the value for **<portkey>** is one of the supported port name keywords (listed below).

The currently supported **<portkey>** values are: **domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

To specify the match condition as a range, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first. The optional **[not]** parameter

has the effect of negating this match condition for the class (i.e., match all source layer 4 ports except for those within the range specified here).

The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source layer 4 port numbers except for the one specified here).

- **Default** **None**
- **Format** **match [not] srcI4port {<portkey> | <0-65535> [<0-65535>]}**
- **Mode** **Class-Map Config**

8.4.15 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field of a packet. The VLAN ID is an integer from 1 to 4094. The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all VLAN Identifier values except for what is specified here).

- **Default** **None**
- **Format** **match [not] vlan <1-4094>**
- **Mode** **Class-Map Config**

8.5 Policy Commands

The 'policy' command set is used in DiffServ to define:

- **Traffic Conditioning** Specify traffic conditioning actions (policing, marking, shaping) to apply to traffic classes
- **Service Provisioning** Specify bandwidth and queue depth management requirements of service levels (EF, AF, etc.)

The policy commands are used to associate a traffic class, which was defined by the class command set, with one or more QoS policy attributes. This association is then assigned to an interface in a particular direction to form a service. The user specifies the policy name when the policy is created.

The DiffServ CLI does not necessarily require that users associate only one traffic class to one policy. In fact, multiple traffic classes can be associated with a single policy, each defining a particular treatment for packets that match the class definition. When a packet satisfies the conditions of more than one class, preference is based on the order in which the classes were added to the policy, with the foremost class taking highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes. Note that the only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is policy-map.

8.5.1 bandwidth kbps

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.

Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.


Note: The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

- **Format** **bandwidth kbps <1-4294967295>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type** - Out
- **Incompatibilities** - Expedite (all forms)

8.5.2 bandwidth percent

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100.


Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

 **Note:** The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

- **Format** **bandwidth percent <1-100>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type** - Out
- **Incompatibilities** - Expedite (all forms)

8.5.3 class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The **<classname>** is the name of an existing DiffServ class. Note that this command causes the specified policy to create a reference to the class definition.

 **Note:** The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

- **Format** **class <classname>**
- **Mode** **Policy-Map Config**


8.5.3.1 no class


This command deletes the instance of a particular class and its defined treatment from the specified policy. **<classname>** is the names of an existing DiffServ class. Note that this command removes the reference to the class definition for the specified policy.

- **Format** **no class <classname>**
- **Mode** **Policy-Map Config**

8.5.4 expedite kbps

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.


 **Note:** The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.


 **Note:** The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

- **Format** **expedite kbps <1-4294967295> [1-128]**
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type** - Out
- **Incompatibilities** - Bandwidth (all forms), Shape Peak

8.5.5 expedite percent

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.

 **Note:** The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

 **Note:** The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

- **Format** **expedite percent <1-100> [1-128]**
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type** - Out
- **Incompatibilities** - Bandwidth (all forms), Shape Peak

8.5.6 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value. The **<dscpval>** value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef**.

- **Format** **mark ip-dscp <dscpval>**
- **Mode** **Policy-Class-Map Config**
- **Policy Type** - In
- **Incompatibilities** - Mark IP Precedence, Police (all forms)

8.5.7 mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

- **Format** **mark ip-precedence <0-7>**
- **Mode** **Policy-Class-Map Config**
- **Policy Type** - In
- **Incompatibilities** - Mark IP DSCP, Police (all forms)

8.5.8 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format** `police-simple {<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscptransmit <0-63> | transmit}]}`
- **Mode** Policy-Class-Map Config
- **Restrictions** - Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type** - In
- **Incompatibilities** - Mark IP DSCP, Mark IP Precedence

8.5.9 police-single-rate

This command is used to establish the traffic policing style for the specified class. The single-rate form of the police command uses a single data rate and two burst sizes, resulting in three outcomes: conform, exceed and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The exceeding burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the exceeding burst size must be equal to or greater than the conforming burst size.

For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this singlerate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format** `police-single-rate {<1-4294967295> <1-128> <1-128> conformaction {drop | set-prec-transmit <0-7> | set-dscp-transmit <0- 63> | transmit} exceed-action {drop |`


```
set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit] [violate-action {drop |
set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit}]}
```

- **Mode** Policy-Class-Map Config
- **Restrictions** - Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type** - In
- **Incompatibilities** - Mark IP DSCP, Mark IP Precedence

8.5.10 police-two-rate

This command is used to establish the traffic policing style for the specified class. The two-rate form of the police command uses two data rates and two burst sizes, resulting in three outcomes: conform, exceed and violate. The first two data parameters are the conforming data rate and burst size. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295, while the conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The next two data parameters are the peak data rate and burst size. The peak data rate is specified in kilobits-persecond (Kbps) as an integer from 1 to 4294967295, while the peak burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the peak data rate must be equal to or greater than the conforming data rate.

For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**


For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format** police-two-rate {<1-4294967295> <1-128> <1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} exceed-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit}]}
- **Mode** Policy-Class-Map Config
- **Restrictions** - Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type** - In
- **Incompatibilities** - Mark IP DSCP, Mark IP Precedence

8.5.11 policy-map

This command establishes a new DiffServ policy. The <policyname> parameter is a case-sensitive

alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to either the inbound or outbound traffic direction as indicated by the {in | out} parameter.

 **Note:** The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

 **Note:** The CLI mode is changed to Policy-Map Config when this command is successfully executed.

- **Format** **policy-map <polycyname> {in | out}**
- **Mode** **Global Config**

8.5.11.1 no policy-map

This command eliminates an existing DiffServ policy. The <polycyname> parameter is the name of an existing DiffServ policy. This command may be issued at any time; if the policy is currently referenced by one or more interface service attachments, this deletion attempt shall fail.

- **Format** **no policy-map <polycyname>**
- **Mode** **Global Config**

8.5.12 policy-map rename


This command changes the name of a DiffServ policy. The <polycyname> is the name of an existing DiffServ class. The <newpolycyname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

- **Format** **policy-map rename <polycyname> <newpolycyname>**
- **Mode** **Global Config**

8.5.13 randomdrop

This command changes the active queue depth management scheme from the default tail drop to RED. The first two data parameters are the average queue depth minimum and maximum threshold values specified in bytes. The minimum threshold is an integer from 1 to 250000. The maximum threshold is an integer from 1 to 500000, but it must be equal to or greater than the minimum threshold. The third data parameter is the maximum drop probability and is an integer from 0 to 100. It indicates the percentage likelihood that a packet will be dropped when the average queue depth reaches the maximum threshold value.


The remaining parameters are all optional. The fourth data parameter is the sampling rate, indicating the period at which the queue is sampled for computing the average depth. Expressed in microseconds, the sampling rate is an integer from 0 to 1000000, with a default of 0 (meaning per-packet sampling). The last parameter is the decay exponent, which determines how quickly the average queue length calculation decays over time, with a higher number producing a faster rate of decay. This value is an integer from 0 to 16, with a default of 9.

 **Note:** The last two parameters, namely sampling rate and decay exponent, are hierarchically specified in this command. That is, in order to provide a value for the decay exponent <0-16>, the user is required to also specify a sampling rate <0-1000000> for proper command interpretation.

- **Format** **randomdrop** <1-250000> <1-500000> <0-100> [<0-1000000> [<0-16>]]
- **Mode** **Policy-Class-Map Config**
- **Policy Type** - Out

8.5.14 shape bps-average


This command is used to establish average rate traffic shaping for the specified class, which limits transmissions for the class to the committed information rate, with excess traffic delayed via queuing. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.

 **Note:** Queue depth management defaults to tail drop, but the randomdrop command can be used to change to a RED scheme.

- **Format** **shape bps-average** <1-4294967295>
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - This shaping rate must not exceed the maximum link data rate of the interface to which the policy is applied.
- **Policy Type** - Out

8.5.15 shape bps-peak

This command is used to establish peak rate traffic shaping for the specified class, which allows transmissions for the class to exceed the committed information rate by sending excess traffic with the understanding that it could be dropped by a downstream network element. Two rate parameters are used, a committed information rate and a peak information rate. Each of these rates is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The peak rate must be specified as equal to or greater than the committed rate.

 **Note:** Queue depth management defaults to tail drop, but the randomdrop command can be used to change to a RED scheme.

- **Format** **shape bps-peak** <1-4294967295> <1-4294967295>
- **Mode** **Policy-Class-Map Config**
- **Restrictions** - Neither of the shaping rate parameters is allowed to exceed the maximum link data rate of the interface to which the policy is applied.
- **Policy Type** - Out
- **Incompatibilities** - Expedite (all forms)

8.6 Service Commands

The 'service' command set is used in DiffServ to define:

- **Traffic Conditioning** Assign a DiffServ traffic conditioning policy (as specified by the policy commands) to an interface in the incoming direction
- **Service Provisioning** Assign a DiffServ service provisioning policy (as specified by the policy commands) to an interface in the outgoing direction


The service commands attach a defined policy to a directional interface. Only one policy may be assigned at any one time to an interface in a particular direction. The policy type (in, out) must match the interface direction to which it is attached.

This set of commands consists of service addition/removal.

The CLI command root is **service-policy**

8.6.1 service-policy

This command attaches a policy to an interface in a particular direction. The command can be used in the **Interface Config** mode to attach a policy to a specific interface. Alternatively, the command can be used in the **Global Config** mode to attach this policy to all system interfaces. The direction value is either in or out. The **<policyname>** parameter is the name of an existing DiffServ policy, whose type must match the interface direction. Note that this command causes a service to create a reference to the policy.


 **Note:** This command effectively enables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

Note: This command shall fail if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition such that it would result in a violation of said interface capabilities shall cause the policy change attempt to fail.

- **Format** **service-policy {in | out} <polycymapname>**
- **Modes** **Global Config (for all system interfaces)**
Interface Config (for a specific interface)
- **Restrictions** Only a single policy may be attached to a particular interface in a particular direction at any one time.

8.6.1.1 no service-policy

This command detaches a policy from an interface in a particular direction. The command can be used in the Interface Config mode to detach a policy from a specific interface. Alternatively, the command can be used in the Global Config mode to detach this policy from all system interfaces to which it is currently attached. The direction value is either in or out. The **<policyname>** parameter is the name of an existing DiffServ policy. Note that this command causes a service to remove its reference to the policy.

 **Note:** This command effectively disables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

- **Format** **no service-policy {in | out} <policyname>**
- **Modes** **Global Config (for all system interfaces)**
 Interface Config (for a specific interface)

8.7 Show Commands

The 'show' command set is used in DiffServ to display configuration and status information for:

- **Classes**
- **Policies**
- **Services**

This information can be displayed in either summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled; it is suppressed otherwise.

There is also a 'show' command for general DiffServ information that is available at any time.

8.7.1 show class-map

This command displays all configuration information for the specified class. The <classname> is the name of an existing DiffServ class.

- **Format** **show class-map [<classname>]**
- **Mode** **Privileged EXEC and User EXEC**

If the Class Name is specified the following fields are displayed:

- **Class Name** - The name of this class.
- **Class Type** - The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
- **Match Criteria** - The Match Criteria fields will only be displayed if they have been configured. They will be displayed in the order entered by the user. These are evaluated in accordance with the class type. The possible Match Criteria fields are: Class of Service, Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, Source Layer 4 Port, Source MAC Address, and VLAN.
- **Values** - This field displays the values of the Match Criteria.
- **Excluded** - This field indicates whether or not this Match Criteria is excluded.

If the Class Name is not specified, this command displays a list of all defined DiffServ classes. The

following fields are displayed:

- **Class Name** - The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
- **Class Type** - The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
- **ACL Number** - The ACL number used to define the class match conditions at the time the class was created. This field is only meaningful if the class type is acl. (Note that the contents of the ACL may have changed since this class was created.)
- **Ref Class Name** - The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

8.7.2 show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

- **Format** **show diffserv**
- **Mode** **Privileged EXEC**
- **DiffServ Admin mode** - The current value of the DiffServ administrative mode.
- **Class Table Size** - The current number of entries (rows) in the Class Table.
- **Class Table Max** - The maximum allowed entries (rows) for the Class Table.
- **Class Rule Table Size** - The current number of entries (rows) in the Class Rule Table.
- **Class Rule Table Max** - The maximum allowed entries (rows) for the Class Rule Table.
- **Policy Table Size** - The current number of entries (rows) in the Policy Table.
- **Policy Table Max** - The maximum allowed entries (rows) for the Policy Table.
- **Policy Instance Table Size** - The current number of entries (rows) in the Policy Instance Table.
- **Policy Instance Table Max** - The maximum allowed entries (rows) for the Policy Instance Table.
- **Policy Attribute Table Size** - The current number of entries (rows) in the Policy Attribute Table.
- **Policy Attribute Table Max** - The maximum allowed entries (rows) for the Policy Attribute Table.
- **Service Table Size** - The current number of entries (rows) in the Service Table.
- **Service Table Max** - The maximum allowed entries (rows) for the Service Table.

8.7.3 show policy-map

This command displays all configuration information for the specified policy. The <policyname> is the name of an existing DiffServ policy.

- **Format** **how policy-map [<policyname>]**
- **Mode** **Privileged EXEC**

If the Policy Name is specified the following fields are displayed:

- **Policy Name** - The name of this policy.
- **Type** - The policy type, namely whether it is an inbound or outbound policy definition.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

- **Class Name** - The name of this class.
- **Mark CoS** - Denotes the class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark cos was not specified.
- **Mark IP DSCP** - Denotes the mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified using the police-two-rate command, or if policing is in use for the class under this policy.
- **Mark IP Precedence** - Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if precedence is not specified using police-tworate command, or if either mark DSCP or policing is in use for the class under this policy.
- **Policing Style** - This field denotes the style of policing, if any, used (simple, single rate, or two rate).
- **Committed Rate (Kbps)** - This field displays the committed rate, used in simple policing, single-rate policing, and two-rate policing.
- **Committed Burst Size (KB)** - This field displays the committed burst size, used in simple policing, single-rate policing, and two-rate policing.
- **Excess Burst Size (KB)** - This field displays the excess burst size, used in single-rate policing.
- **Peak Rate (Kbps)** - This field displays the peak rate, used in two-rate policing.
- **Peak Burst Size (KB)** - This field displays the peak burst size, used in two-rate policing.
- **Conform Action** - The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
- **Conform DSCP Value** - This field shows the DSCP mark value if the conform action is markdscp.
- **Conform IP Precedence Value** - This field shows the IP Precedence mark value if the conform action is markprec.
- **Exceed Action** - The current setting for the action taken on a packet considered to exceed to the policing parameters. This is not displayed if policing not in use for the class under this policy.
- **Exceed DSCP Value** - This field shows the DSCP mark value if this action is markdscp.
- **Exceed IP Precedence Value** - This field shows the IP Precedence mark value if this action is markprec.
- **Non-Conform Action** - The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.

- **Non-Conform DSCP Value** - This field displays the DSCP mark value if this action is markdscp.
- **Non-Conform IP Precedence Value** - This field displays the IP Precedence mark value if this action is markprec.
- **Bandwidth** - This field displays the minimum amount of bandwidth reserved in either percent or kilobits-per-second.
- **Expedite Burst Size (KBytes)** - This field displays the maximum guaranteed amount of bandwidth reserved in either percent or kilobits-per-second format.
- **Shaping Average** - This field is displayed if average shaping is in use. Indicates whether average or peak rate shaping is in use, along with the parameters used to form the traffic shaping criteria, such as CIR and PIR. This is not displayed if shaping is not configured for the class under this policy.
- **Shape Committed Rate (Kbps)** - This field is displayed if average or peak rate shaping is in use. It displays the shaping committed rate in kilobits-per-second.
- **Shape Peak Rate (Kbps)** - This field is displayed if peak rate shaping is in use. It displays the shaping peak rate in kilobits-per-second.
- **Random Drop Minimum Threshold** - This field displays the RED minimum threshold. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Maximum Threshold** - This field displays the RED maximum threshold. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Maximum Drop Probability** - This field displays the RED maximum drop probability. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Sampling Rate** - This field displays the RED sampling rate. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Decay Exponent** - This field displays the RED decay exponent. This is not displayed if the queue depth management scheme is not RED.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

- **Policy Name** - The name of this policy. (Note that the order in which the policies are displayed is not necessarily the same order in which they were created.)
- **Policy Type** - The policy type, namely whether it is an inbound or outbound policy definition.
- **Class Members** - List of all class names associated with this policy.

8.7.4 show diffserv service

This command displays policy service information for the specified interface and direction. The <slot/port> parameter specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

- **Format** **show diffserv service <slot/port> {in | out}**
- **Mode** **Privileged EXEC**

- **DiffServ Admin Mode** - The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
- **Interface** - The slot number and port number of the interface (slot/port).
- **Direction** - The traffic direction of this interface service, either in or out.
- **Operational Status** - The current operational status of this DiffServ service interface.
- **Policy Name** - The name of the policy attached to the interface in the indicated direction.
- **Policy Details** - Attached policy details, whose content is identical to that described for the show policy-map <policyname> command (content not repeated here for brevity).

8.7.5 show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The direction parameter is optional; if specified, only services in the indicated direction are shown, otherwise service information is shown for both directions, where applicable.

- **Format** `show diffserv service brief [in | out]`
- **Mode** **Privileged EXEC**
- **DiffServ Mode** - The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Interface - The slot number and port number of the interface (slot/port).

Direction - The traffic direction of this interface service, either in or out.

OperStatus - The current operational status of this DiffServ service interface.

Policy Name - The name of the policy attached to the interface in the indicated direction.

8.7.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The <slot/port> parameter specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

 **Note:** This command is only allowed while the DiffServ administrative mode is enabled.


- **Format** `show policy-map interface <slot/port> <in | out>`
- **Interface** - The slot number and port number of the interface (slot/port).
- **Direction** - The traffic direction of this interface service, either in or out.
- **Operational Status** - The current operational status of this DiffServ service interface.
- **Policy Name** - The name of the policy attached to the interface in the indicated direction.
- **Interface Offered Octets/Packets** - A cumulative count of the octets/packets offered to this service interface in the specified direction before the defined DiffServ treatment is applied.
- **Interface Discarded Octets/Packets** - A cumulative count of the octets/packets discarded by this

service interface in the specified direction for any reason due to DiffServ treatment.

- **Interface Sent Octets/Packets** - A cumulative count of the octets/packets forwarded by this service interface in the specified direction after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element.

The following information is repeated for each class instance within this policy:

- **Class Name** - The name of this class instance.
- **In Offered Octets/Packets** - A count of the octets/packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.
- **In Discarded Octets/Packets** - A count of the octets/packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. Only displayed for the 'in' direction.
- **Tail Dropped Octets/Packets** - A count of the octets/packets discarded due to tail dropping from a transmission queue, typically due to the effects of traffic shaping. These counts may not be supported on all platforms. Only displayed for the 'out' direction.
- **Random Dropped Octets/Packets** - A count of the octets/packets discarded due to WRED active queue depth management, typically due to the effects of traffic shaping. These counts are only applicable for a class instance whose policy attributes includes random dropping, and may not be supported on all platforms. Only displayed for the 'out' direction.
- **Shape Delayed Octets/Packets** - A count of the octets/packets that were delayed due to traffic shaping. These counts are only applicable for a class instance whose policy attributes includes shaping, and may not be supported on all platforms. Only displayed for the 'out' direction.
- **Sent Octets/Packets** - A count of the octets/packets forwarded for this class instance after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element. Only displayed for the 'out' direction.

 **Note:** None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

8.7.7 show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction. The direction parameter indicates the interface direction of interest.


This command enables or disables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are enable and disable.

- **Format** `show service-policy [in | out]`
- **Mode** `Privileged EXEC`

The following information is repeated for each interface and direction (only those interfaces configured

with an attached policy are shown):

- **Interface** - The slot number and port number of the interface (slot/port).
- **Dir** - The traffic direction of this interface service, either in or out.
- **Operational Status** - The current operational status of this DiffServ service interface.
- **Offered Packets** - A count of the total number of packets offered to all class instances in this service before their defined DiffServ treatment is applied. These are overall per-interface perdirection counts.
- **Discarded Packets** - A count of the total number of packets discarded for all class instances in this service for any reason due to DiffServ treatment. These are overall per-interface perdirection counts.
- **Sent Packets** - A count of the total number of packets forwarded for all class instances in this service after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element. These are overall per-interface per-direction counts.
- **Policy Name** - The name of the policy attached to the interface.

 **Note:** None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

8.8 Rate-Limiting Commands

8.8.1 rate-limiting

This command is used to set the bandwidth of a specified interface. The type of rate limiting is specific to either the inbound or outbound traffic direction as indicated by the **{ingress | egress}** parameter. The **<limit>** parameter defines the value of bandwidth in megabit-per-second (Mbps). The granularity of bandwidth for the 10/100 interface is 1 Mbps and for the gigabit interface is 8 Mbps.

- **Format** **rate-limiting {ingress | egress} <limit>**
- **Mode** **Interface Config**

8.8.1.1 no rate-limiting

This command removes the bandwidth limitation of specified interface.

- **Format** **no rate-limiting {ingress | egress}**
- **Mode** **Interface Config**

8.8.2 show rate-limiting

This command displays the bandwidth of limiting in both ingress and egress direction for one or all interface

- **Format** **show rate-limiting {<slot/port> | all}**

- **Mode** **Privileged EXEC and User EXEC**

9. CLI COMMANDS: SECURITY

9.1 Security Commands

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

9.1.1 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**

9.1.1.1 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 'authentication login'. The default login list cannot be deleted.
- **Format** **no authentication login <listname>**
- **Mode** **Global Config**

9.1.2 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

9.1.3 clear radius statistics

This command is used to clear all RADIUS statistics.

- **Format** clear radius statistics
- **Mode** Privileged EXEC

9.1.4 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

9.1.5 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

9.1.6 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

9.1.7 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

9.1.7.1 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**

9.1.8 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**

9.1.8.1 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**

9.1.9 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**

9.1.9.1 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**

9.1.10 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**

9.1.11 dot1x re-authentication

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

- **Default** **Disabled**
- **Format** **dot1x re-authentication**
- **Mode** **Interface Config**

9.1.11.1 no dot1x re-authentication

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

- **Format** **no dot1x re-authentication**
- **Mode** **Interface Config**

9.1.12 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**

9.1.12.1 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**

9.1.13 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**

9.1.13.1 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**

9.1.14 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**

9.1.14.1 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**

9.1.15 radius accounting mode

This command is used to enable the RADIUS accounting function.

- **Default** **Disabled**
- **Format** **radius accounting mode**
- **Mode** **Global Config**

9.1.15.1 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** **lobal Config**

9.1.16 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** **lobal Config**

9.1.16.1 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**

9.1.17 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**

9.1.18 radius server msgauth

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

- **Default** **radius server msgauth <ipaddr>**
- **Mode** **Global Config**

9.1.19 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**

9.1.20 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**

9.1.20.1 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**

9.1.21 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**

9.1.21.1 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**

9.1.22 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.

9.1.23 show authentication

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

- **Format** `show authentication`
- **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.

9.1.24 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** `show authentication users <listname>`
- **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.

9.1.25 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** `show dot1x [{summary {<slot/port> | all}] | {detail <slot/port>} | {statistics`

<slot/port>}]

- **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.

9.1.26 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.

9.1.27 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

9.1.28 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 filed 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.

9.1.29 show users authentication

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

- **Format** **show users authentication**
- **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.

9.1.30 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** `users defaultlogin <listname>`
- **Mode** `Global Config`

9.1.31 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** `users login <user> <listname>`
- **Mode** `Global Config`

9.2 Secure Shell (SSH) Commands

The commands in this section is not supported currently

9.2.1 ip ssh

This command is used to enable SSH.

- **Default** `Disabled`
- **Format** `ip ssh`
- **Mode** `Privileged EXEC`

9.2.1.1 no ip ssh

This command is used to disable SSH.

- **Format** `no ip ssh`
- **Mode** `Privileged EXEC`

9.2.2 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** `ip ssh protocol [1] [2]`
- **Mode** `Privileged EXEC`

9.2.3 show ip ssh

This command displays the ssh settings.

- **Format** **show ip ssh**
- **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.

9.3 HTTP Commands

The commands in this section is not supported currently

9.3.1 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** **ip http secure-port <portid>**
- **Mode** **Privileged EXEC**

9.3.1.1 no ip http secure-port

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

- **Format** **no ip http secure-port**
- **Mode** **Privileged EXEC**

9.3.2 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** **ip http secure-protocol [SSL3] [TLS1]**
- **Mode** **Privileged EXEC**

9.3.2.1 no ip http secure-protocol

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

- **Format** **no ip http secure-protocol [SSL3] [TLS1]**
- **Mode** **Privileged EXEC**

9.3.3 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**

9.3.3.1 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**

9.3.4 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**

9.3.4.1 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**

9.3.5 show ip http

This command displays the http settings for the switch.

- **Format** **show ip http**
- **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.

9.4 MAC Lock Commands

9.4.1 mac-lock

This command adds the specified MAC address with **<vlanid>** to a specified interface. The **<macaddr>** parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The **<vlanid>** parameter must identify a valid VLAN.

- **Format** **mac-lock <vlanid> <macaddr>**
- **Mode** **Interface Config**

9.4.1.1 no mac-lock

This command removes the MAC address with the MAC address of **<macaddr>** and VLAN of **<vlanid>** locked by the specified interface.

- **Format** **mac-lock <vlanid> <macaddr>**
- **Mode** **Interface Config**

9.4.2 show mac-lock

This command displays the vlan id and mac addresses that are locked at the specified interface for one or all interfaces.

- **Format** **show mac-lock {<slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

10. CLI COMMANDS: SWITCHING

10.1 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.

10.1.1 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** - Configured 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)

10.1.2 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.

10.1.3 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.

10.1.4 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** - 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.

10.1.5 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.

10.1.6 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.

10.1.7 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** - Configured 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

10.1.8 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

10.1.9 spanning-tree

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

- **Default** **Disabled**
- **Format** **spanning-tree**
- **Mode** **Global Config**

10.1.9.1 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**

10.1.10 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**

10.1.10.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

- **Format** **no spanning-tree configuration name**
- **Mode** **Global Config**

10.1.11 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**

10.1.11.1 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**

10.1.12 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**

10.1.12.1 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**

10.1.13 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**

10.1.13.1 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**

10.1.14 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 $(\text{Bridge Max Age} / 2) + 1$.

- **Default** **15**
- **Format** **spanning-tree forward-time <4-30>**
- **Mode** **Global Config**

10.1.14.1 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**

10.1.15 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 $(\text{Bridge Max Age} / 2) - 1$.

- **Default** **2**
- **Format** **spanning-tree hello-time <1-10>**
- **Mode** **Global Config**

10.1.15.1 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**

10.1.16 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 $2 \times (\text{Bridge Forward Delay} - 1)$.

- **Default** **20**

- **Format** **spanning-tree max-age <6-40>**
- **Mode** **Global Config**

10.1.16.1 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**

10.1.17 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**

10.1.17.1 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**

10.1.18 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 this switch is 4.

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

10.1.18.1 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**

10.1.19 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**

10.1.19.1 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**

10.1.20 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**

10.1.20.1 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**

10.1.21 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**

10.1.21.1 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**

10.1.22 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**

10.1.22.1 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**

11. USING THE WEB INTERFACE

This chapter is a brief introduction to the web. You can manage your switch through a Web browser and Internet connection. This is referred to as Web-based management. To access the switch, the Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript(TM) version 1.2, or later

This section explains how to access the switch Web-based management panels to configure and manage the switch.

It is important to note that there are equivalent functions in the Web interface as in the terminal interface (that is, there are usually the same menus to accomplish a task). For example, when you log in, there is a Main Menu with the same functions available, and so on. To terminate the Web login session, close the web browser.

There are several differences between the Web and terminal interfaces. For example, on the Web interface the entire forwarding database can be displayed, and the terminal interface only displays 10 entries starting at specified addresses.

11.1 Configuring for Web Access

To enable Web access to the switch:

1. Configure the switch for in-band connectivity.
2. Enable HTTP Web mode. For layer 2, see 'ip http server' command.

11.1.1 Web Page Layout

A Web interface panel for the switch Web page consists of three frames (Figure 12).

Frame 1, across the top, displays a led panel of the switch.

Frame 2, at the middle displays tab and sub-menu of categorized figuration command.

Frame 3, the bottom frame, displays the currently selected device configuration status or the user configurable information that you have selected from the tree view of Frame 2, or both.

The screenshot shows the PLANET Web Management Interface. At the top left is the PLANET logo. Below it is a navigation tree with folders for System, Switching, Security, and QOS. The main content area is titled 'System Description' and contains the following information:

System Description	24-Port Ethernet Security Switch
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
IP Address	192.168.0.100
System Object ID	M7
System Up Time	0 days, 0 hours, 21 minutes
MIBs Supported	RFC 1907 - SNMPv2-MIB RFC 2819 - RMON-MIB MGMTSW-REF-MIB MGMTSW-DHCP-MIB SNMP-COMMUNITY-MIB SNMP-FRAMEWORK-MIB SNMP-MPD-MIB SNMP-NOTIFICATION-MIB SNMP-TARGET-MIB SNMP-USER-BASED-SM-MIB

11.1.2 Starting the Web Interface

Note: You must configure the IP address of the switch before using the Web interface.

Follow these steps to bring up the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed, enter the appropriate User Name and Password. The User Name and associated password are the same ones used for the terminal interface. Click on the Login button. The navigation tree is displayed in Frame 2, and the System Description Menu is displayed in Frame 3.
3. Make your selection by clicking on the appropriate item in the navigation tree in Frame 2.

11.1.3 Command Buttons

The following command buttons are used throughout the Web interface panels for the switch:

- **Save** Implements and saves the changes you just made. Some settings may require you to reset the system in order for them to take effect.
- **Refresh** The Refresh button that appears next to the Apply button in Web interface panels refreshes the data on the panel.
- **Submit** Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

12. SWITCH OPERATION

12.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

12.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

12.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

12.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is

subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

12.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

13. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

Some stations cannot talk to other stations located on the other port

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

Performance is bad

Solution:

Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

Why the Switch doesn't connect to the network

Solution:

- Check the LNK/ACT LED on the switch
- Try another port on the Switch
- Make sure the cable is installed properly
- Make sure the cable is the right type
- Turn off the power. After a while, turn on power again

APPENDIX A

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

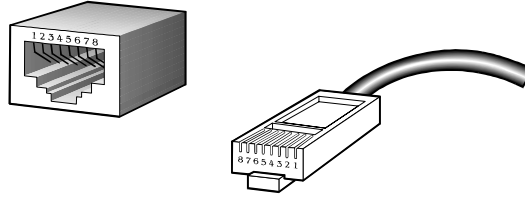
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

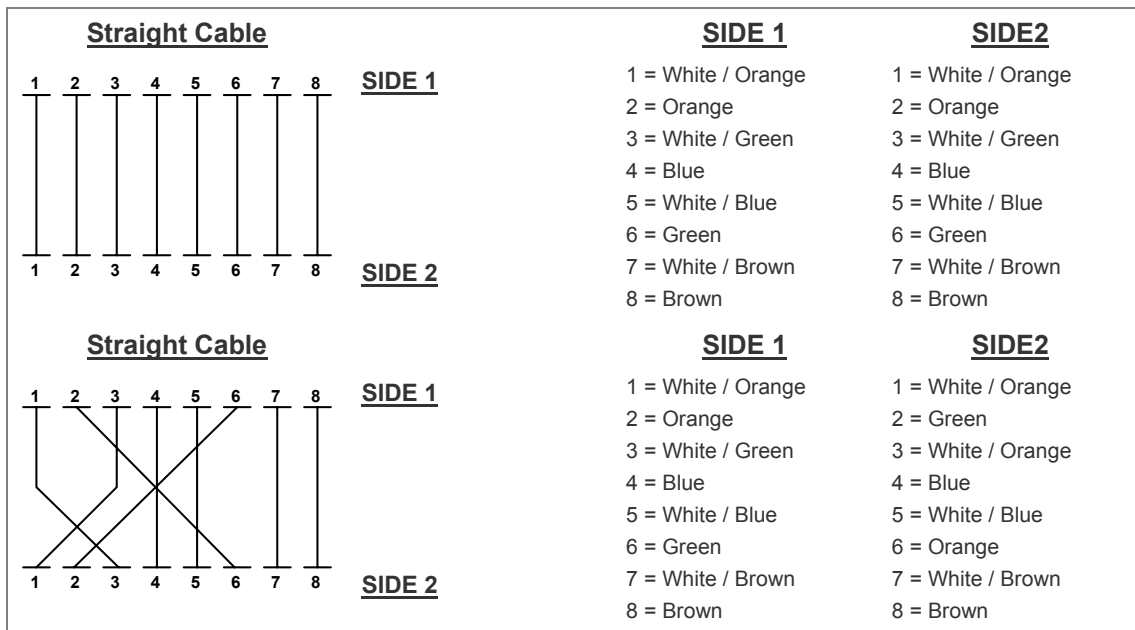


Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.